SMART GRID INTEROPERABILITY PANEL

Guide for Assessing the High-Level Security Requirements in NISTIR 7628

SGIP Document Number: CSWG-TC-001, Version 0.10
Document Source: July 23, 2012
Author/Editor: SGIP CSWG – Test & Certification Subgroup
Production Date: July 23, 2012

RIGHT TO DISTRIBUTE AND CREDIT NOTICE

DISCLAIMER

This document is a work product of the SGIP. It was prepared by the participants of the SGIP and approved by the Smart Grid Interoperability Panel's Plenary Leadership. Neither the National Institute of Standards and Technology (NIST), the SGIP leadership, its members nor any person acting on behalf of any of the above:

- *MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, process, or composition disclosed in this report may not infringe on privately owned rights; or*
- *Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, process, or composition disclosed in this report.*
- *Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Smart Grid Interoperability Panel.*

THIS IS NOT A NIST DOCUMENT

THE SGIP

The Smart Grid Interoperability Panel (SGIP) is a membership-based organization created by an Administrator under a contract from NIST to provide an open process for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration, and harmonization of standards development for the Smart Grid. The SGIP also reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Smart Grid testing and certification, and proposes action plans for achieving these goals. The SGIP does not write standards, but serves as a forum to coordinate the development of standards and specifications by many standards-setting organizations.

Contents

Tables

Figures

1. Executive Summary

Guide for Assessing the High-Level Security Requirements in NISTIR 7628 provides a set of guidelines for building effective security assessment plans and a baseline set of procedures for assessing the effectiveness of security requirements employed in Smart Grid information systems.[1] This guide is written to provide a foundation to facilitate a security assessment based on the National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, high-level security requirements implemented within an effective risk management program. The intended audience for this guide is any individual or group responsible for developing and/or assessing an organization's security posture against the requirements in NISTIR 7628.

This guide is organized as follows:

- **Section One** is an introduction that includes the purpose, NISTIR 7628 background information, and the target audience.
- **Section Two** describes three basic concepts needed when assessing the high-level requirements in Smart Grid information systems.
- **Section Three** describes the Security Assessment process, including specific activities carried out in each phase of the assessment.
- **Section Four and Five** include the revision history and contributors.
- **Appendix A** describes the assessment method definitions tailored from NIST Special Publication (SP) 800-53 A, Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans.*
- **Appendix B** contains the Assessment Procedures Catalog.

In addition, the Assessment Procedures Catalog of Appendix B has been placed in a companion spreadsheet for assessors that can be used to record the findings of an assessment and used as the basis for the development of a final assessment report.

The objective of security assessments is to verify that the implementers and operators of Smart Grid information systems are meeting their stated goals. The security assessment process involves participation and buy-in from both the assessor and organizational stakeholders. Key organizational participants in the process include senior management, Smart Grid information system and industrial control system owners, and the Chief Information Security Officer.

[1] For this document, Smart Grid information system implies information technology (IT) and /or industrial control systems (ICS).

The result of the security assessment provides realistic information to senior management about the risk posture and residual risks of the Smart Grid information system, which will form the basis for any decision to approve or authorize the system for operation.

2. Introduction

As the transition to the Smart Grid occurs, the electricity sector becomes increasingly dependent on information technology (IT)[2] (i.e., hardware, software, and firmware), processes, industrial control systems (ICSs),[3] and people, working together to provide organizations with the capability to process, store, and transmit information and commands in a timely manner to support various missions and business functions. The degree to which organizations depend upon IT systems and ICSs[4] to conduct routine, important, and critical mission and business functions means that the protection of the underlying systems is paramount to the success of the organization.

The selection of appropriate security requirements for Smart Grid information systems is an important task that can have major implications on the operations and assets of an organization. Security requirements are the management, operational, and technical safeguards or countermeasures prescribed for Smart Grid information systems to protect the confidentiality, integrity, and availability of the system and its information. Once employed, security requirements are assessed to gather the information necessary to determine overall effectiveness of the requirements; that is, the extent to which the requirements are implemented correctly, operating as intended, and producing the desired security posture for the Smart Grid information system. Understanding the overall effectiveness of the security requirements implemented in the Smart Grid information system and its operational environment is essential in determining the risk to the organization's operations.

This Assessment Guide shows organizations how to develop and conduct a baseline assessment program[5] to determine compliance with the National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, published in August 2010, which documents high-level security requirements in volume one.[6] A companion spreadsheet for assessors has been developed that can be used to record the findings of an assessment. This Assessment Guide also defines key participants, their roles, responsibilities, and major considerations that should be a part of

[2] IT is a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate (i.e., people, processes, technologies, and facilities).

[3] ICS is a set of hardware and software acting in concert that manages the behavior of other devices in the electrical grid.

[4] For this document, the term Smart Grid information system implies IT systems and/or ICS.

[5] Appendix B provides an assessment procedure catalog that allows an organization to customize requirements, assessment objectives, assessment methods, and assessment objects for an organization Smart Grid information system specific assessment.

[6] http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

any security assessment on NISTIR 7268 compliance.[7] Figure 1 depicts the four-phase security assessment process that is described in detail in Chapter 3.

Finally, any security assessment using this Assessment Guide should inform the organization's senior management of the major security risks levels with respect to the availability, integrity, and confidentiality of both physical and informational Smart Grid system assets evaluated.

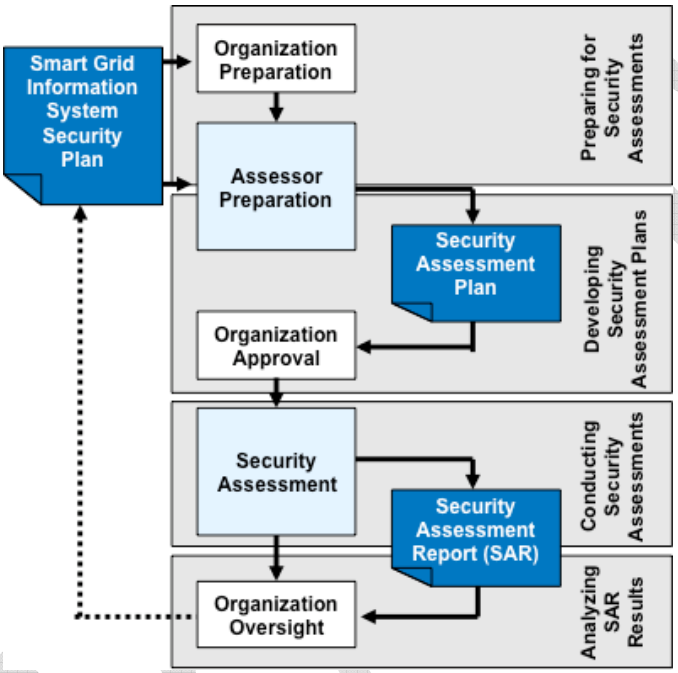

Figure 1. Smart Grid Security Assessment Process

2.1 Purpose

Security assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits. Rather, they are the principal vehicle used to verify that the implementers and operators of Smart Grid information systems including the telecommunications infrastructures are meeting their stated security goals and objectives.

This Assessment Guide provides advice and tips to those conducting a security assessment of Smart Grid information systems based on NISTIR 7628 high-level security requirements. A well-executed and written security assessment provides realistic information to senior management about the residual risks of the Smart Grid information system, which will

[7] Neither NISTIR 7628 nor this Guide imposes any actual requirements on any person or entity. The application of any "requirements" in NISTIR 7628 or any "assessment" thereof pursuant to this Guide will be self-imposed, imposed by contract between the relevant parties or imposed by the applicable regulatory authority if and to the extent determined to be so imposed.

form the basis for any decision to approve or authorize the system for operation. The security assessment should provide senior management with:

- An overview of the threat landscape and vulnerabilities to their Smart Grid information system in terms of confidentiality, integrity and availability;
- Evidence of the validity of the effectiveness of security requirements and implementation described in the Smart Grid information systems cybersecurity plan;[8]
- An indication of the quality of the risk management processes employed within the organization;
- Information about the strengths and weaknesses of Smart Grid information systems which are supporting critical missions and applications in a global environment of sophisticated threats; and
- Recommendations for administrative and technical security measures to reduce risks to acceptable levels.

A major challenge for those assessing Smart Grid security is establishing which major security objectives (confidentiality, integrity, and availability) are the most important for a specific system. There is no "one size fits all" as each Smart Grid information system may contain physical and information assets that touch on all three security objectives. For example, a Smart Grid information system that consists of assets that deal with automated metering and communication between a utility and residential customers may place a premium on securing the integrity and the confidentiality of the information for billing and privacy reasons. In contrast, a Smart Grid information system that is heavily focused on generation and transmission will probably place a very high priority on the availability of electric power and information on load and take steps to promote availability and reliability.

Those individuals who conduct security assessments (Assessors) of Smart Grid information systems must address the above challenges and communicate the security assessment's findings in terms of confidentiality, integrity and availability

2.2 NISTIR 7628 Background

The three-volume report, *Guidelines for Smart Grid Cyber Security* (NISTIR 7628), presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. The electricity sector is a diverse community of stakeholders—from utilities to providers of energy management services, to manufacturers of electric vehicles and charging stations.

[8] Cybersecurity plan development outlines are provided by organizations such as National Rural Electric Cooperative Association (NRECA) and NIST, i.e., NIST Special Publication (SP) 800-18, Rev 1, *Guide for Developing Security Plans for Federal Information Systems*.

Any electricity sector enterprise can adopt, partially or in full, the methods and supporting information presented in the NISTIR 7628 as normative requirements for assessing their cybersecurity risk, and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively isolated system to a complex, highly interconnected environment. As the electric grid continues to evolve, each organization's cybersecurity requirements should progress as technology advances and threats to grid security multiply and diversify.

The three volumes that make up NISTIR 7628 are intended primarily for individuals and organizations responsible for addressing Smart Grid information system cybersecurity. As a result of the pervasiveness of the electric power infrastructure and its growing importance in the U.S. economy, these individuals and organizations comprise a large and diverse group that includes vendors of energy information and management services, equipment manufacturers, utilities, system operators, regulators, researchers, and network specialists. In addition, NISTIR 7628 incorporates the perspectives of three primary industries converging on opportunities enabled by the emerging Smart Grid—utilities and other businesses in the electricity sector, the information technology industry, and the telecommunications sector. NISTIR 7628 describes the approach, including the risk assessment process, used by the SGIP Cyber Security Working Group (CSWG) to identify high-level security requirements. It also presents a high-level architecture followed by a sample logical interface reference model used to identify and define logical interface categories and across the seven Smart Grid domains. High-level security requirements for each of the logical interface categories are then described.

2.3 Target Audience

This guide is intended for any individuals or groups responsible for developing and assessing an organization's high-level security posture against the requirements in NISTIR 7628. The Smart Grid electricity sector is becoming increasing complex with multiple players. It will include information security and industrial control system professionals in traditional electric utilities, merchant power generators, transmission companies, Regional Transmission Organizations, Independent System Operators, national and regional electric reliability organizations as well as providers of energy management services, manufacturers of electric vehicles, and charging stations

This guide intends to serve a diverse group of Smart Grid information system and information security professionals, including individuals responsible for:

- Industrial control system professionals responsible for day-to-day safe and secure operation of power generation, transmission, and distribution assets (e.g., utility staff, Supervisory Control And Data Acquisition (SCADA) and ICS hardware and software vendors, SCADA and ICS security hardware and software, and systems integrators;
- Information system and security requirement assessment and monitoring (e.g., system evaluators, assessors/assessment teams, certification agents/certification

teams, independent verification and validation assessors, auditors, , information system owners);

- Information system and security management and oversight (e.g., senior information security officers, information security managers);
- Information security implementation and operation (e.g., information system owners, mission / business owners, and information system security officers); and
- Information system development and integration (e.g., program managers, information technology product developers, information system developers, systems integrators).

2.4 Roles and Responsibilities

Smart Grid security assessments involve individuals with the following roles and responsibilities:[9]

1. Senior management of the organization;
2. Chief Information Security Officer (CISO) and information security staff;
3. Smart Grid information system owners; and
4. Assessors who will prepare and conduct the assessment.

Senior management has the overall responsibility of approving the scope of the Smart Grid security assessment and ensuring that organizational staff cooperates with the assessors. Prior to finalizing the security assessment plan, senior management reviews and approves the plan. Ultimately, senior management also approves the final security assessment report and any measures to bring the Smart Grid information system to acceptable risk levels with respect to the high-level security requirements of NISTIR 7628.

CISOs are responsible for balancing security needs with the organization's strategic business plan, and acting as the primary liaison between senior management of the organization and information system owners. In collaboration with Smart Grid information systems owners, the CISO and Information Security staff determines which security requirements are to be assessed for partial assessments.

The Smart Grid information system owners work closely with assessors throughout the security assessment process, acting as the primary point of contact in the organization for the assessors. They review the initial (draft) security assessment report and may correct any weaknesses/deficiencies in the implementation of the security requirements or correct/clarify interpretations of assessment results prior to the delivery of the final report. With the concurrence of designated organizational officials, which may include senior management, the CISO, and information security staff, the Smart Grid information system owners determine the steps to correct weaknesses/deficiencies identified during

[9] Organizations may define other roles for the security assessment process within their organization. It is recognized that individuals may fill multiple roles, though caution should be exercised to ensure no conflict of interest.

the assessment.

Assessors are responsible for preparing the scope of the assessment, developing the security assessment plan with input from organizational staff, and selecting the appropriate procedures to be used in assessing the security requirements. Assessors must obtain approval from senior management prior to executing the assessment. They are also responsible for communicating the degree of compliance of existing and proposed security measures and delivering an initial (draft) and the final security assessment report to the Smart Grid information system owners.

3. Cybersecurity Assessment Fundamentals

This chapter describes the three basic concepts needed when assessing the high-level security requirements in Smart Grid information systems: (i) identifying the high-level security requirements; (ii) security assessment objectives; and (iii) assessment methods and the corresponding assessment objects.

3.1 Identifying the High-Level Security Requirements

The Smart Grid information system's cybersecurity plan describes the high-level security requirements in place or planned for that system. NISTIR 7628 describes high-level security requirements that are applicable to the entire Smart Grid or to particular domains, such as generation or distribution, and interface categories. Power system operations pose many security challenges that are different from the challenges faced by most other industries and within power system operational environments. In particular, there are strict performance and reliability requirements that power system operations need to meet. The requirements in NISTIR 7628 that help to ensure performance and reliability needs were selected from a larger collection of requirements reviewed by the CSWG.[10]

Each of the high-level security requirements is assigned to one of the three categories where a particular requirement is most applicable within an organization, operation, or function. The categories are:

- ***Governance, risk, and compliance (GRC) requirements:*** Addresses requirements at the Smart Grid organizational level;
- ***Common technical requirements:*** Applicable to all interfaces; and
- ***Unique technical requirements:*** Applicable to zero or more—but not all—interfaces. Some of these requirements are not assigned to an interface category, but exist for the readers' consideration.

The common and unique technical requirements should be allocated to each Smart Grid information system, but not necessarily to every component[11] within a system, as the focus is on system-level security and not on specific information exchanges between components. Each organization should develop a security architecture for each Smart Grid information system and allocate appropriate security requirements. Some security requirements may be allocated to one or more Smart Grid information systems. Impact

[10] Sources include NIST SP 800-53A, Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*; Department of Homeland Security Catalog of Control Systems Security: Recommendations for Standards Developers; NERC Critical Infrastructure Protection Standards (CIPS); and Nuclear Regulatory Commission Regulatory Guidance.

[11] Components include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors, field bus, and control network), operating systems, middleware, applications, programmable logic controller hardware, remote terminal unit, actuators, diagnostics, and intelligent electronic devices.

levels[12] for a specific Smart Grid information system—and, therefore, the need to implement requirement enhancements to specific requirements— will be determined by organizations during the risk assessment process.

In addition, organizations may find it necessary to identify compensating security requirements. A compensating security requirement is implemented by an organization in lieu of a recommended security requirement to provide an equivalent or comparable level of protection for the Smart Grid information system and the information processed, stored, or transmitted by that Smart Grid information system. More than one compensating requirement may be necessary to provide the equivalent or comparable protection for a particular security requirement. For example, an organization with significant staff limitations may compensate for the recommended separation of duty security requirement by strengthening the audit, accountability, and personnel security requirements within the Smart Grid information system.

Each NISTIR 7628 high-level security requirement is presented in a standard format with the following information:

- *Security requirement identifier and name.* Each security requirement has a unique identifier that consists of three components. The initial component is SG – for Smart Grid. The second component is the family name, e.g., AC for Access Control and CP for Continuity of Operations. The third component is a unique numeric identifier, for example, SG.AC-1 and SG.CP-3. Each requirement also has a unique descriptive name.
- *Category.* This identifies whether the security requirement is a GRC, common technical, or unique technical requirement. For each common technical security requirement, the most applicable objective (confidentiality, integrity, and availability) is listed.
- The *Requirement* describes specific security-related activities or actions to be carried out by the organization or by the Smart Grid information system.
- The *Supplemental Guidance* section provides additional information that may be useful in understanding the security requirement.
- The *Requirement Enhancements* section provides additional capability to (i) build additional functionality to a requirement, and/or (ii) increase the strength of a requirement. In both cases, the requirement enhancements are to be considered in Smart Grid information systems requiring greater protection due to the potential impact of hardware or data loss based on the results of a risk assessment. Requirement enhancements are numbered sequentially within each requirement.
- The *Additional Considerations* provide additional statements of security capability that may be used to enhance the associated security requirement. These are provided for organizations to consider as they implement Smart Grid information systems and are not intended as security requirements. Each additional

[12]The three impact levels, i.e., low, moderate, and high, are based upon the expected adverse effect of a security breach upon organizational operations, assets, or individuals. NISTIR 7628, Section 3.3 Impact Levels for the confidentiality, integrity, and availability (CI&A) categories, provides additional information.

352 consideration is numbered A1, A2, etc., to distinguish them from the security
353 requirements and requirement enhancements.
354 • The *Impact Level Allocation* identifies the security requirement and associated
355 enhancements, as applicable, at each impact level: low, moderate, and high. The
356 impact levels for a specific Smart Grid information system will be determined by the
357 organization in the risk assessment process.
358
359 **Table 1. Sample NISTIR 7628 high-level security requirement, SG.MP-3, Media Marking**

SG.MP-3 Media Marking

Category: Common Governance, Risk, and Compliance (GRC) Requirements

Requirement
The organization marks removable Smart Grid information system media and Smart Grid information system output in accordance with organization-defined policy and procedures.

Supplemental Guidance
Smart Grid information system markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the Smart Grid information system). External markings are distinguished from internal markings (i.e., the labels used on internal data structures within the Smart Grid information system).

Requirement Enhancements
None.

Additional Considerations
None.

Impact Level Allocation

Low: Not Selected	Moderate: SG. MP-3	High: SG. MP-3

360

361 *3.2 Security Assessment Objectives*

362 An assessment procedure consists of a set of assessment objectives, each with an
363 associated set of potential assessment methods and objects. An assessment
364 objective includes a set of determination statements related to the particular
365 security requirement[13] being assessed. The determination statements are closely
366 linked to the content of NISTIR 7628 high-level security requirements to ensure
367 traceability of assessment results back to a fundamental requirement. The
368 application or execution of an assessment procedure to a security requirement
369 produces assessment findings. These assessment findings are subsequently used to
370 help determine the overall effectiveness of the security requirements, i.e., whether
371 the requirement is implemented and if so, providing the desired outcome.
372
373 The assessment objectives identify the following items to be assessed:
374
375 • **Specifications** are the document-based artifacts (e.g., policies, procedures, plans,
376 system security requirements, functional specifications, and architectural designs)
377 associated with a Smart Grid information system.

[13] Security requirements under assessment also include any requirement enhancements.

- **Mechanisms** are the specific hardware, software, or firmware safeguards and countermeasures employed within a Smart Grid information system.[14]
- **Activities** are the specific protection-related pursuits or actions supporting a Smart Grid information system that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising a contingency plan).
- **Individuals**, or groups of individuals, are people applying the specifications, mechanisms, or activities described above to the Smart Grid information system.

Table 2 depicts the assessment objective that corresponds with the sample NISTIR 7628 high-level security requirement, SG.MP-3.

Table 2. SG.MP-3, Media Marking Assessment Objective

Assessment Objective: SG. MP-3.1
Determine if: (i) The organization documents the storage requirements of stored media; (ii) The organization physically manages Smart Grid information system media within protected areas; and (iii) The organization physically stores Smart Grid information system media within protected areas.

3.3 Assessment Methods

The assessment methods consist of examine, interview, and test, and define the nature of the assessor actions. An Assessor may use any or all of the assessment methods listed below:

- The **examine** method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence.
- The **interview** method is the process of conducting discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence.
- The **test** method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

In all three assessment methods, the results are used to make specific determinations, thereby achieving the objectives of the assessment procedure. Appendix A displays the definitions of the assessment methods provided by NIST SP 800-53A, Rev 1, and adopted for the NISTIR 7628 assessment process. Table 3 illustrates the corresponding assessment methods for the sample NISTIR 7628 high-level security requirement and assessment objective.

[14] Mechanisms also include physical protection devices associated with a Smart Grid information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes, etc.).

414 **Table 3. SG.MP-3, Media Marking Assessment Method**

SG.MP-3.1	***Assessment Objective:*** *Determine if:* *(i) The organization documents the storage requirements of stored media;* *(ii) The organization physically manages Smart Grid information system media within protected areas; and* *(iii) The organization physically stores Smart Grid information system media within protected areas.* **Potential Assessment Methods and Objects:** **Examine:** [SELECT FROM: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records]. **Interview:** [SELECT FROM: Organizational personnel with information system media protection and marking responsibilities]. **Test:** [SELECT FROM: Automated mechanisms supporting removable media marking; media checking process for markings on removable media; removable media].

415
416 Each of the assessment methods described has a set of associated attributes, depth and
417 coverage, which help to define the expected level of effort needed to carry out the
418 assessment. These attributes are hierarchical in nature, providing the means to define the
419 assessment rigor and scope for the increased assurance needed for higher impact level
420 Smart Grid information systems.
421
422 • The **depth** attribute addresses the rigor of and level of detail in the examination,
423 interview, and testing processes. The depth attribute is expressed using the values
424 of generalized, focused, and detailed.
425 • The **coverage** attribute addresses the scope or breadth of the examination,
426 interview, and testing processes including the number and type of specifications,
427 mechanisms, and activities to be examined or tested and the number and types of
428 individuals to be interviewed. The coverage attribute is expressed using the values
429 representative, specific, and comprehensive.
430
431 Within NISTIR 7628, each of the Smart Grid information system impact levels (i.e., low,
432 moderate, and high) has an associated set of minimum assurance requirements. Based on
433 the assurance requirements, security requirement developers and implementers can carry
434 out required activities as an inherent part of developing or implementing the requirement,
435 thereby producing the necessary requirement documentation, conducting essential
436 analyses, and defining actions that must be performed during operation.[15] The purpose of

[15] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security requirements within a Smart Grid information system. This may include, for example, hardware and software vendors providing the requirements, contractors implementing the requirements, or organizational personnel such as Smart Grid information system owners, system

these activities is to provide increased grounds for confidence that the security requirements are implemented correctly, operating as intended, and producing the desired outcome.

The minimum assurance requirements in NISTIR 7628 help to establish an appropriate set of expectations for assessors when conducting the security requirement assessments. The assessment expectations are based on a Smart Grid information systems impact level – low, moderate, or high – for a range of assessment objects including specifications, activities, and mechanisms.

An organization should tailor the assessment procedures to match the characteristics of the Smart Grid information system under assessment. The tailoring process provides organizations with the flexibility needed to avoid security assessment approaches that are unnecessarily extensive or more rigorous than necessary. Supplementation involves adding assessment procedures or assessment details to adequately meet the organization's risk management needs (e.g., adding assessment objectives or adding organization-specific details such as system/platform-specific information for selected security requirements). Supplementation decisions are left to the discretion of the organization in order to maximize flexibility in developing security assessment plans[16] when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments. While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration.

security officers, system and network administrators, or other individuals with security responsibility for the Smart Grid information system.

[16] See Chapter 3 for information on assessment plan development.

4. Security Assessment Process

This chapter describes the process of assessing the security requirements in Smart Grid information systems including: (i) the activities carried out by organizations and assessors to prepare for security requirement assessments, (ii) the development of security assessment plans, (iii) the conduct of security requirement assessments and the analysis, documentation, and reporting of assessment results, and (iv) post-assessment report analysis and follow-on activities carried out by organizations.

The output and end result of the security requirement assessment is the security assessment report, which documents the assurance cases[17] for the Smart Grid information system. This report includes information from the assessor (in the form of assessment findings) to inform senior management on the effectiveness of the security requirements implemented in the Smart Grid information system.

4.1 Preparing for Security Assessments

Successful security requirement assessments depend on the cooperation and collaboration among all parties having a vested interest in the organization's information and ICS security posture. Key participants should include Smart Grid information system owners, senior management, and ICS operators. ICS staff is especially critical when power generation, transmission, and distribution are part of the Smart Grid information system being analyzed, because recommended potential assessment criteria and techniques may have adverse effects on the safety and reliability of Smart Grid assets and systems.

Establishing an appropriate set of expectations before, during, and after the assessment is paramount to achieving an acceptable outcome—that is, producing information necessary to help organizational officials make a credible, risk-based decision on whether to place a Smart Grid information system into operation, continue its operation, or determine which mitigations to implement first. Thorough preparation by the organization and the assessors is an important aspect of conducting effective security requirement assessments. Preparatory activities address a range of issues relating to the cost, schedule, and performance of the assessment.

An organization's key activities, when preparing for a security requirement assessment, include:

- Ensuring that appropriate policies covering security requirement assessments are in place and understood by all affected organizational elements;
- Ensuring that security requirements have been assigned to appropriate organizational entities for development and implementation;
- Establishing the objective and scope of the security requirement assessment (i.e., the *purpose* of the assessment and what is being assessed);

[17] An assurance case is a structured set of arguments and a body of evidence showing that a Smart Grid system satisfies specific claims with respect to a given quality attribute.

- Notifying key organizational officials of the impending assessment and allocating necessary resources to carry out the assessment;
- Establishing appropriate communication channels among organizational officials having an interest in the assessment;
- Establishing time frames for completing the assessment and key milestone decision points required by the organization to effectively manage the assessment;
- Identifying and selecting a competent assessor/assessment team that will be responsible for conducting the assessment, considering issues of assessor independence;
- Collecting artifacts to provide to the assessor/assessment team. Examples of artifacts include policies, procedures, plans, specifications, designs, records, administrator/operator manuals, Smart Grid information system documentation, interconnection agreements, previous assessment results, etc.; and
- Establishing a mechanism between the organization and the assessor to minimize ambiguities or misunderstandings about security requirement implementation or security requirement weaknesses/deficiencies identified during the assessment.

Assessors' key activities, when preparing for a security requirement assessment, include:

- Obtaining a general understanding of the organization's operation (including mission, functions, and business processes) and how the Smart Grid information system to be assessed supports those organizational operations;
- Obtaining an understanding of the structure of the information system (i.e., system architecture);
- Obtaining a thorough understanding of the security requirements being assessed;
- Establishing appropriate organizational points of contact needed to carry out the assessment;
- Obtaining artifacts needed for the assessment (see the example artifacts listed above for the organization's activities);
- Obtaining previous assessment results that may be appropriately reused for the current assessment;
- Meeting with appropriate organizational officials to ensure common understanding for assessment objectives and the proposed rigor and scope of the assessment; and
- Developing a security assessment plan.[18]

[18] Additional guidance on preparing for cybersecurity requirement assessments can be found in Section 3.1 of NIST SP 800-53A.

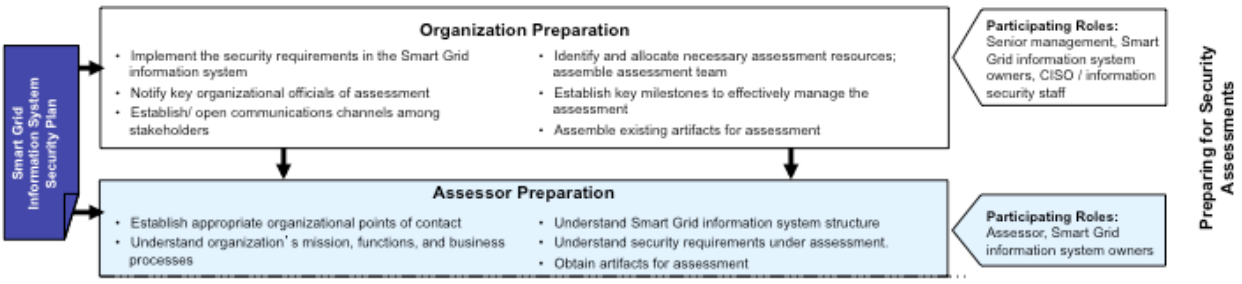

Figure 2. Preparing for Security Assessments

4.2 Developing Security Assessment Plans

The security assessment plan developed by the Assessor provides the objectives for the security requirement assessment and a detailed roadmap of how to conduct such an assessment.

Assessors should consider the following steps when developing plans to assess the security requirements for Smart Grid information systems:

- Determine which security requirements/requirement enhancements are to be included in the assessment based on the contents of the security plan and the purpose/scope of the assessment (i.e., where "scope" refers to a complete or partial assessment);
- Select the appropriate assessment procedures to be used during the assessment based on the security requirements and requirement enhancements;
- Tailor the selected assessment procedures for the Smart Grid information system impact level and organization's operating environment;
- Optimize the assessment procedures to reduce duplication of effort and provide cost-effective assessment solutions; and
- Finalize the assessment plan and obtain the necessary approvals to execute the plan.

4.2.1 Determine which security requirements are to be assessed

The cybersecurity system plan developed by the assessor provides an overview of the security requirements for the Smart Grid information system and describes the security requirements to be assessed. The assessor starts with the security requirements described in the security plan and considers the purpose of the assessment. A security requirement assessment can be either a complete or partial assessment of the security requirements implemented in the Smart Grid information system. Complete assessments address all implemented security requirements.

For partial assessments, Smart Grid information system owners collaborate with organizational officials (e.g., chief information security officers, asset owners, mission/information owners, and executive management) to determine which security requirements are to be assessed. The selection of the security requirements to assess depends on the Smart Grid information system owner and the organization to ensure that

requirements with greater volatility or importance to the organization are assessed more frequently, and requirement implementations that have changed since the last assessment are reevaluated.[19]

4.2.2 Select appropriate procedures to assess the security requirements

Appendix B, Assessment Procedures Catalog, is a table that contains examples of assessment procedures for each security requirement and requirement enhancement in NISTIR 7628. For each security requirement and requirement enhancement in the security plan to be included in the assessment, assessors select the corresponding assessment procedure from the spreadsheet.

4.2.3 Tailor assessment procedures for specific operating environments

The assessment procedures listed in Appendix B are tailored to meet specific organizational needs, in a manner similar to how the security requirements from NISTIR 7628 are tailored for the organization's mission, business functions, characteristics of the Smart Grid information system, and operating environment. Assessment procedures can be tailored by:

- Selecting the assessment methods and objects needed to satisfy assessment objectives and most cost-effectively make appropriate determinations;
- Selecting the appropriate depth and coverage attribute values defines the scope and rigor of the assessment to be performed;
- Eliminating assessment procedures for common security requirements if those requirements have been assessed by another documented assessment process;
- Developing Smart Grid information system-specific assessment procedures;
- Incorporating assessment results from previous assessments, where the results are deemed applicable; and
- Making appropriate adjustments in assessment procedures to be able to obtain the requisite assessment evidence from external providers.

4.2.4 Optimize selected assessment procedures to ensure maximum efficiency

Assessors have a great deal of flexibility in selecting assessment methods and organizing a security assessment plan that meets the needs of the organization and provides the best opportunity for obtaining the necessary evidence to determine the effectiveness of security requirement. Combining and consolidating assessment procedures is one area where this flexibility can be applied. During the assessment of a Smart Grid information system, assessment methods are applied numerous times to a variety of assessment objects within a particular family of security requirements. To save time, reduce assessment costs, and maximize the usefulness of assessment results, assessors should review the selected assessment procedures for the security requirement families and combine or consolidate the procedures (or parts of procedures) whenever possible or practicable.

[19] NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidance on continuous monitoring as part of the risk management process.

4.2.5 Finalize security assessment plan and obtain approval to execute plan

After completing the preceding steps, the security assessment plan is finalized and the schedule is established including key milestones for the assessment process. Once the security assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials to ensure that the plan is complete, consistent with the security objectives of the organization and the organization's assessment of risk, and cost-effective with regard to the resources allocated for the assessment.

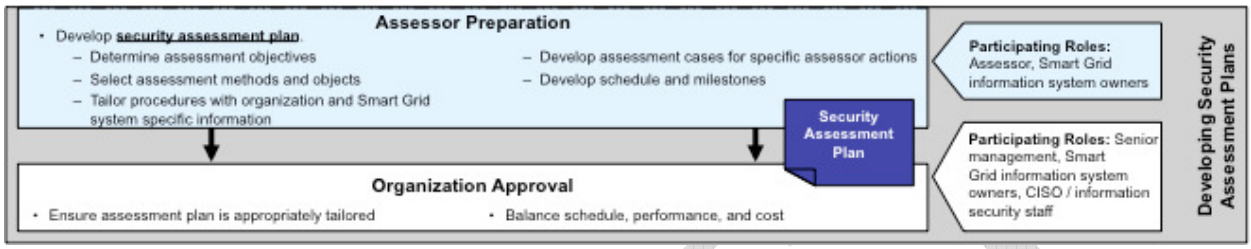

Figure 3. Developing Security Assessment Plans

4.3 Conducting Security Requirement Assessments

After the security assessment plan is approved in writing by the organization's senior management, the assessor executes the plan in accordance with the agreed-upon milestones and schedule. Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the information necessary to make the determination associated with each assessment objective.

Assessors prepare determination statements which are accompanied by finding(s) on whether or not the security requirements are meeting specific objectives. Assessors may express their findings as described below or may use other terms:

- **Satisfied (S).** The assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the requirement has been met producing a fully acceptable result.
- **Other than satisfied (O).** The assessment information obtained indicates potential anomalies in the operation or implementation of the requirement that may need to be addressed by the organization. A finding of other than satisfied may also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient information to make the particular determination called for in the determination statement.

However, the assessor organization may have a more robust lexicon for expressing their findings.

The Smart Grid information system owner relies on the assessor's security expertise and technical judgment to: (i) assess the security requirements in the Smart Grid information system; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the requirements and reduce or eliminate identified vulnerabilities. The

assessor provides this information to the Smart Grid information system owner in the initial (draft) security assessment report. If there are specific opportunities to correct weaknesses or deficiencies in the security requirements or to correct/clarify misunderstandings or interpretations of assessment results, then the Smart Grid information system owner may choose to act on selected recommendations before the security assessment report is finalized. Security requirements modified, enhanced, or added during this process should be reassessed by the assessor prior to the production of the final security assessment report. The delivery of the final assessment report to the Smart Grid information system owner marks the official end of the security requirement assessment.

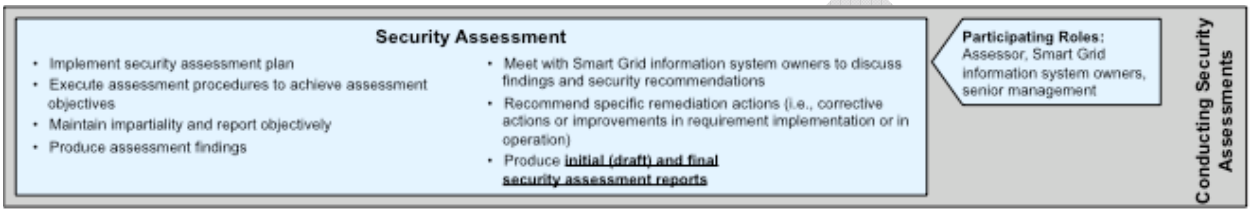

Figure 4. Conducting Security Requirement Assessments

4.4 Analyzing Security Assessment Report Results

Since results of the security requirement assessment ultimately influence the content of the security plan, the Smart Grid information system owner reviews the security assessment report. Then with the concurrence of designated organizational officials, the Smart Grid information system owner determines the appropriate steps required to correct weaknesses and deficiencies identified during the assessment. By using the tags of "Satisfied" and "Other than Satisfied," the reporting format for the assessment findings provides visibility for organizational officials into specific weaknesses and deficiencies in the Smart Grid information system and facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities.

Senior management involvement in the mitigation process is necessary to ensure that the organization's resources are effectively allocated in accordance with organizational priorities and risk posture. Senior management first provides resources to the Smart Grid information systems that : (i) support the most critical and sensitive missions for the organization, or (ii) correct the deficiencies that pose the greatest degree of risk. Ultimately, the assessment findings and any subsequent mitigation actions initiated by the Smart Grid information system owner in collaboration with designated organizational officials trigger updates to the risk assessment and the security plan.

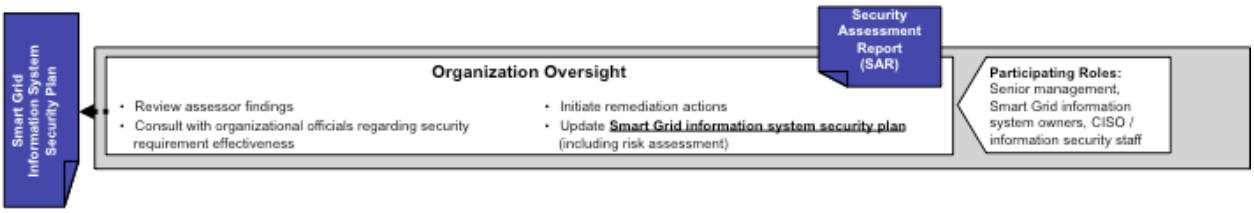

Figure 5. Analyzing Security Assessment Report Results

Figure 6 provides an overview of the security requirement assessment process, including the activities carried out during pre-assessment, assessment, and post-assessment.

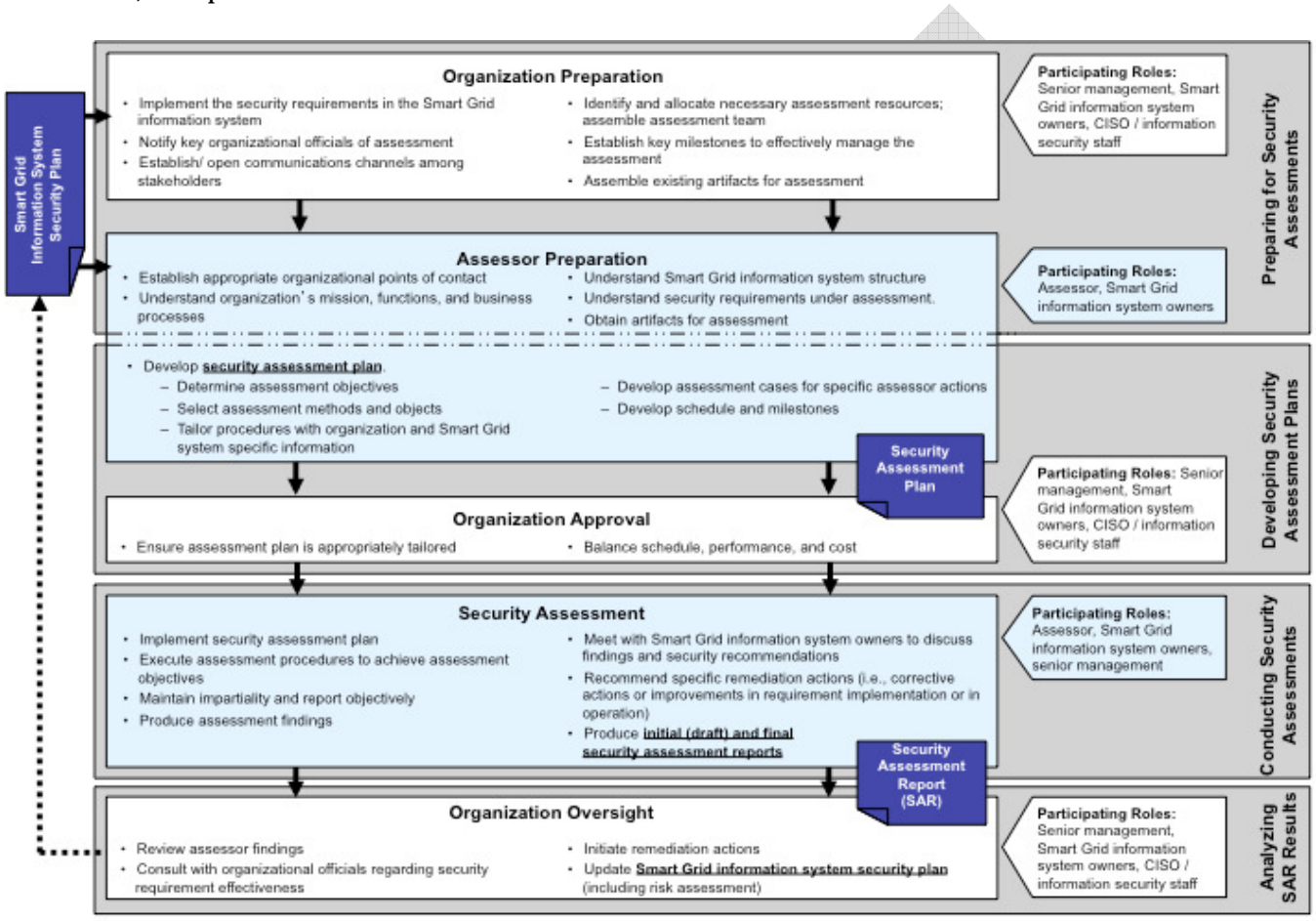

Figure 6. Smart Grid Security Requirement Assessment Process Overview [20]

[20] This figure was adapted from Figure 1-Security Control Assessment Process Overiew of NIST SP 800-53A, Rev 1: *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans* (See http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf).

5. Revision History

SGIP Document Number: CSWG-TC-001, Version 0.8

THIS IS NOT A NIST DOCUMENT

Rev. Number	Date	Author/Editor	Summary of Revisions
0.3	8/15/2011	CSWG TCC	Initial document
0.4 – 0.8	09/15/2011 – 11/21/2011	CSWG Management Team	Comments and updates

6. Contributors

Thank you to the following members of the CSWG and CSWG Security Testing and Certification Subgroup for their contributions in developing this document:

- Mike Ahmadi
- Sandy Bacik
- Richard Bockenek
- James Foti
- Nelson Hastings
- Michaela Iorga
- Stan Kladko
- Victoria Yan Pillitteri
- Scott Shorter
- Marianne Swanson

Appendix A – NIST SP800-53A Assessment Method Definitions

ASSESSMENT METHOD	ASSESSMENT OBJECTS	DEFINITION	SUPPLEMENTAL GUIDANCE
Examine	Specifications (e.g., policies, plans, procedures, system requirements, designs) Mechanisms (e.g., functionality implemented in hardware, software, firmware) Activities (e.g., system operations, administration, management, exercises)	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.	Typical assessor actions may include, for example: • reviewing information security policies, plans, and procedures; • analyzing system design documentation and interface specifications; • observing system backup operations, reviewing the results of contingency plan exercises; • observing incident response activities; • studying technical manuals and user/administrator guides; • checking, studying, or observing the operation of an information technology mechanism in the Smart Grid information system hardware/software; and • checking, studying, or observing physical security measures related to the operation of a Smart Grid information system.
Interview	Individuals or groups of individuals.	The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time. Surveys and questionnaires can be used in advance of discussions to help frame and streamline the discussion process.	Typical assessor actions may include, for example interviewing: • agency heads; • chief information officers; • senior agency information security officers; • authorizing officials; • information owners; • Smart Grid information system and mission owners; • Smart Grid information system security officers; • Smart Grid information system security managers; • personnel officers; • human resource managers; • facilities managers; • training officers; • Smart Grid information system operators; • network and system administrators; • site managers; • physical security officers; and • users.
Test	Mechanisms (e.g., hardware, software, firmware) Activities (e.g., system operations, administration, management; exercises)	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.	Typical assessor actions may include, for example: • testing access control, identification and authentication, and audit mechanisms; • testing security configuration settings; • testing physical access control devices; conducting penetration testing of key Smart Grid information system components; • testing Smart Grid information system backup operations; • testing incident response capability; and • exercising contingency planning capability.

Appendix B – Assessment Procedures Catalog

The Smart Grid cybersecurity requirements identified below are from the NISTIR 7628, *Guidelines for Smart Grid Cyber Security, Volume 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.*

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
Access Control (SG.AC)				
SG.AC-1	Access Control Policy and Procedures	SG.AC-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the access control security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented access control security policy that addresses— (I) the objectives, roles, and responsibilities for the access control security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the access control security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the access control security policy and associated access control protection requirements. SG. AC -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. AC -1.3 Determine if the organization ensures that the access control security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Access control policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with access control responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-2	Remote Access Policy and Procedures	SG.AC-2.1 Determine if the organization documents the allowed remote access to the Smart Grid information system. SG.AC-2.2 Determine if the organization establishes usage restrictions and implementation guidance for each allowed remote access method. SG.AC-2.3 Determine if the organization authorizes remote access to the Smart Grid information system prior to connection. SG.AC-2.4 Determine if the organization enforces requirements for remote connections to Smart Grid information systems.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities]. Test: [SELECT FROM: Remote access methods for the Smart Grid information system].
SG.AC-3	Account Management	SG.AC-3.1 Determine if: (i) the organization manages Smart Grid information system accounts, including (a) authorizing; (b) establishing; (c) activating; (d) modifying; (e) disabling; and (f) removing accounts; and (ii) the organization specifies account types, access rights; and privileges. SG.AC-3.2 Determine if: (i) the organization defines the frequency for account reviews; and (ii) the organization reviews accounts in accordance with the organization-defined frequency. SG.AC-3.3 Determine if: the organization notifies account managers when Smart Grid information system users are terminated, transferred; and when Smart Grid information system usage changes. SG.AC-3.4 Determine if the organization requires management approval prior to establishing accounts.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-4	Access Enforcement	SG.AC-4.1 Determine if the Smart Grid information system enforces assigned authorizations for controlling access to the system in accordance with the organizational defined policy.	Examine	Examine: [SELECT FROM: Access control policy; procedures addressing access enforcement; Smart Grid information system configuration settings and associated documentation; list of approved authorizations (user privileges); Smart Grid information system audit records; and other relevant documents or records].
SG.AC-5	Information Flow Enforcement	SG.AC-5.1 Determine if: (i) the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems; (ii) the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; and (iii) the Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with the organizational policy.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing information flow enforcement; Smart Grid information system design documentation; information; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing information flow enforcement policy].
SG.AC-6	Separation of Duties	SG.AC-6.1 Determine if: (i) the organization establishes divisions of responsibility as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; (ii) the organization documents divisions of responsibility duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; (iii) the organization establishes separation of duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and (iv) the organization documents separation of duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. SG.AC-6.2 Determine if the organization enforces separation of smart grid functions through assigned access authorizations. SG.AC-6.3 Determine if the organization restricts security functions to an organizational defined minimum amount of users necessary to ensure the security of the Smart Grid information system.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties]. Test: [SELECT FROM: Automated mechanisms implementing separation of duties policy].
SG.AC-7	Least Privilege	SG.AC-7.1 Determine if the organization assigns the most restrictive set	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing least privilege; list of assigned

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		of rights/privileges or accesses needed by users for the performance of specified tasks. SG.AC-7.2 Determine if the organization configures the Smart Grid information system to enforce the most restrictive set of rights/privileges or accesses needed by users.		access authorization (user privileges); Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].
SG.AC-8	Unsuccessful Login Attempts	SG.AC-8.1 Determine if: (i) the organization defines a limit of consecutive invalid access attempts by a user during an organization-defined time period; (ii) the organization enforces the limit of consecutive invalid access attempts by a user during an organization-defined time period; and (iii) the organization defines the time period for consecutive invalid access attempts by a user.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing unsuccessful login attempts; Smart Grid information system configuration system and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for unsuccessful login attempts].
SG.AC-9	Smart Grid Information System Use Notification	SG.AC-9.1 Determine if: (i) the organization defines a system use notification message/banner for security and privacy for the Smart Grid information system consistent with applicable laws, directives, policies, regulations, standards, and guidance; (ii) the organization documents a system use notification message/banner for security and privacy for the Smart Grid information system; (iii) the organization approves a system use notification message /banner for security and privacy for the Smart Grid information system; and (iv) the Smart Grid information system displays an approved system use notification message/banner for security and privacy before granting Smart Grid information system access.	Examine, Test	Examine: [SELECT FROM: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of Smart Grid information system use notification messages or banners; Smart Grid information system notification messages; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records for user acceptance of notification message or banner; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for system use notification].
SG.AC-10	Previous Logon Notification	SG.AC-10.1 Determine if the Smart Grid information system, upon successful logon, displays the date of the last logon, the time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing previous logon notification; Smart Grid information system configuration settings and associated documentation; Smart Grid information system notification messages; Smart Grid information system design documentation; Smart Grid information system design documentation; Smart Grid information system audit records; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for previous

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				logon notification].
SG.AC-11	Concurrent Session Control	SG.AC-11.1 Determine if: (i) the organization defines the limit of concurrent sessions for any user on the Smart Grid information system; and (ii) the organization enforces the limit of concurrent sessions for any user on the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing concurrent session control; Smart Grid information system configuration settings and associated documentation; security plan; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for concurrent session control].
SG.AC-12	Session Lock	SG.AC-12.1 Determine if: (i) the organization defines the time period of user inactivity after which the Smart Grid information system initiates a session lock; and (ii) the organization enforces the time period of user inactivity after which the Smart Grid information system initiates a session lock of receiving a request from a user. SG.AC-12.2 Determine if the Smart Grid information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing session lock; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; security plan; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for session lock].
SG.AC-13	Remote Session Termination	SG.AC-13.1 Determine if: (i) the organization defines the time period of inactivity before the Smart Grid information system terminates a remote session; and (ii) the Smart Grid information system terminates a remote session at the end of the remote session or after the organizationally defined remote access inactivity period.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing session timing and termination; Smart Grid information system design documentation; organization-defined time period of inactivity before remote session termination; Smart Grid information system configuration settings and associated documentation; security plan; and other relevant documents or records]. Test: [SELECT FROM: Remote session termination capability within the Smart Grid information system].
SG.AC-14	Permitted Actions without Identification or Authentication	SG.AC-14.1 Determine if: (i) the organization identifies specific user actions that can be performed on the Smart Grid information system without identification or authentication; and (ii) the organization documents and provides supporting	Examine	Examine: [SELECT FROM: Access control policy; procedures addressing permitted actions without identification and authentication; Smart Grid information system configuration settings and associated documentation; security plan; list of Smart Grid information system actions that can be

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		rationale for user actions that can be performed on the Smart Grid information system without identification or authentication. SG.AC-14.2 Determine if the organization identifies any actions that normally require identification or authentication but may, under certain organization-defined circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. SG.AC-14.3 (requirement enhancement 1) Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.		performed without identification and authentication; Smart Grid information system audit records; and other relevant documents or records].
SG.AC-15	Remote Access	SG.AC-15.1 Determine if: (i) the organization authorizes remote access to the Smart Grid information system for all allowed methods of remote access; (ii) the organization monitors remote access to the Smart Grid information system for all allowed methods of remote access; and (iii) the organization manages remote access to the Smart Grid information system for all allowed methods of remote access. SG.AC-15.2 (requirement enhancement 1) Determine if: (i) the organization authenticates remote access; and (ii) the organization uses cryptography to protect the confidentiality and integrity of remote access sessions; SG.AC-15.3 (requirement enhancement 2) Determine if: (i) the organization defines a limited number of managed access control points for remote access to the Smart Grid information system; and (ii) the Smart Grid information system controls all remote access through a limited number of managed access control points. SG.AC-15.4 (requirement enhancement 3) Determine if: (i) the organization defines the protection of wireless access to the Smart Grid information system using authentication and encryption; and	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; Smart Grid information system audit records; list of managed access control points; other relevant documents or records; procedures addressing wireless implementation and usage (including restrictions); and wireless scanning reports]. Interview: [SELECT FROM: Organizational personnel responsible for remote access authorization, monitoring, and control; and organizational personnel responsible for monitoring wireless connections to the Smart Grid information system]. Test: [SELECT FROM: Remote access methods for the Smart Grid information system; Automated mechanisms implementing the access control policy for remote access; automated mechanisms implementing cryptographic protections for remote access; automated mechanisms implementing access control policy for wireless access of the Smart Grid information system; and scanning procedures for detecting unauthorized wireless access points and connections].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the Smart Grid information system uses authentication and encryption to protect wireless access. SG.AC-15.5 (requirement enhancement 4) Determine if: (i) the organization monitors for unauthorized remote connections to the Smart Grid information system and takes appropriate action if an unauthorized connection is discovered; (ii) the organization defines a frequency for scanning wireless access points; (iii) the organization defines actions for unauthorized wireless connections to the Smart Grid information system; and (iv) the organization enforces the actions for unauthorized wireless connections to the Smart Grid information system.		
SG.AC-16	Wireless Access Restrictions	SG.AC-16.1 Determine if the organization establishes use restrictions and implementation guidance for wireless technologies. SG.AC-16.2 Determine if: (i) the organization authorizes wireless access to the Smart Grid information system; (ii) the organization monitors wireless access to the Smart Grid information system; and (iii) the organization manages wireless access to the Smart Grid information system.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel responsible for authorizing, monitoring, or controlling the use of wireless technologies in the Smart Grid information system]. Test: [SELECT FROM: Wireless access usage and restrictions].
SG.AC-17	Access Control for Portable and Mobile Devices	SG.AC-17.1 Determine if: (i) the organization establishes usage restrictions for organization-controlled portable and mobile devices, including the use of writeable, removable media and personally owned removable media; and (ii) the organization establishes implementation guidance for organization-controlled portable and mobile devices, including the use of writeable, removable media and personally owned removable media. SG.AC-17.2 Determine if the organization authorizes connections of mobile devices to the Smart Grid information system.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing access control for portable and mobile devices; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel who use portable and mobile devices to access the Smart Grid information system]. Test: [SELECT FROM: Automated mechanisms implementing access control policy for portable and

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.AC-17.3 Determine if the organization monitors for unauthorized connections of mobile devices to the Smart Grid information system. SG.AC-17.4 Determine if: (i) the organization documents requirements for the connection of mobile devices to the Smart Grid information system; and (ii) the organization enforces requirements for the connection of mobile devices to the Smart Grid information system. SG.AC-17.5 (requirement enhancement 1) Determine if: (i) the organization documents the use of writable, removable media in Smart Grid information systems; and (ii) the organization controls the use of writable, removable media in Smart Grid information systems. SG.AC-17.6 (requirement enhancement 2) Determine if: (i) the organization documents the use of personally owned removable media in Smart Grid information systems; and (ii) the organizations controls the use personally owned removable media in Smart Grid information systems. SG.AC-17.7 (requirement enhancement 3) Determine if: (i) the organization documents the configuration of mobile devices assigned to individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; (ii) the organization maintains the organizationally defined configured mobile devices to be assigned to individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; and (iii) the organization issues organizationally defined configured mobile devices to be assigned to individual travel to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures. SG.AC-17.8 (requirement enhancement 4)		mobile devices].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if: (i) the organization documents measures on mobile devices returning from locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; and (ii) the organization enforces measures on mobile devices returning from locations that the organization determines to be of significant risk in accordance with organizational policies and procedures.		
SG.AC-18	Use of External Information Control Systems	SG.AC-18.1 Determine if: (i) the organization documents terms and conditions for authorized individual to access the Smart Grid information system from an external Smart Grid information system; and (ii) the organization identifies individuals authorized to access the Smart Grid information system from external information systems. SG.AC-18.2 Determine if: (i) the organization documents terms and conditions for authorized individuals to process, store, and transmit organization-controlled information using an external Smart Grid information system; and (ii) the organization identifies individuals authorized to process, store, and transmit organization-controlled information using external information systems. SG.AC-18.3 (requirement enhancement 1) Determine if: (i) the organization documents restrictions on authorized individual with regard to the use of organization-controlled removable media on external Smart Grid information systems; and (ii) the organization enforces restrictions on authorized individual with regard to the use of organization-controlled removable media on external Smart Grid information systems.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational Smart Grid information systems].
SG.AC-19	Control System Access Restrictions	SG.AC-19.1 Determine if: (i) the organization documents mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network; (ii) the organization implements mechanisms in the design and implementation of a Smart Grid information system	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing access restriction to the Smart Grid information system and organization's enterprise network; Smart Grid information system configuration settings and associated documentation; enterprise network configuration settings; and enterprise security architecture documentation; other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		to restrict access to the Smart Grid information system from the organization's enterprise network; and (iii) the organization enforces mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network.		Test: [SELECT FROM: Automated mechanisms implementing access restrictions within the Smart Grid information system and enterprise network].
SG.AC-20	Publicly Accessible Content	SG.AC-20.1 Determine if the organization designates individuals authorized to post information onto an organizational Smart Grid information system that is publicly accessible. SG.AC-20.2 Determine if the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information. SG.AC-20.3 Determine if the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational Smart Grid information system. SG.AC-20.4 Determine if the organization reviews the content on the publicly accessible organizational Smart Grid information system for nonpublic information on an organization-defined frequency. SG.AC-20.5 Determine if the organization removes nonpublic information from the publicly accessible organizational Smart Grid information system, if discovered.	Examine, Interview	Examine: [SELECT FROM: Access control policy; policies and procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational Smart Grid information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public Web sites; system audit logs; security awareness training records; Public information policy; Social media policy; procedures for posting publicly available information; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for posting, maintaining, and managing public content posted on organizational Smart Grid information systems].
SG.AC-21	Passwords	SG.AC-21.1 Determine if: (i) the organization develops policies and procedures for Smart Grid information system users concerning the generation and use of passwords; (ii) the organization implements policies and procedures for Smart Grid information system users concerning the generation and use of passwords; and (iii) the organization enforces policies and procedures for Smart Grid information system users concerning the generation and use of passwords. SG.AC-21.2 Determine if the organizational policies document rules of complexity, based on the criticality level of the Smart Grid	Examine, Test	Examine: [SELECT FROM: Password policy; authentication policy; procedures addressing authentication and password control; security plan; list of active system accounts along with the name of the individual associated with each account and the last time the password has been changed; list of guest/anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires and the last time the password was changed; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing password policy management; automated mechanisms for changing passwords; and

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		information system to be accessed. SG.AC-21.3 Determine if: (i) the organizational policies document rules of passwords are changed regularly; and (ii) the organizational policies document rules of passwords are revoked after an extended period of inactivity.		automated mechanisms for password expiration].
Awareness and Training (SG.AT)				
SG.AT-1	Awareness and Training Policy and Procedures	SG.AT-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the awareness and training security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented awareness and training security policy that addresses— (I) the objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the awareness and training security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the awareness and training security policy and associated awareness and training protection requirements. SG. AT -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. AT -1.3 Determine if the organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security awareness and training responsibilities].
SG.AT-2	Security Awareness	SG.AT-2.1 Determine if:	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization provides basic security awareness briefings to all Smart Grid information system users on an organizational defined frequency; and (ii) the organization defines the frequency of security awareness briefings.		awareness training implementation; security awareness training curriculum; security awareness training materials; security plan; training records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel comprising the general Smart Grid information system user community].
SG.AT-3	Security Training	SG.AT-3.1 Determine if: (i) the organization provides security training before authorizing access to the Smart Grid information system; and (ii) the organization provides security training before performing duties for accessing the Smart Grid information system; SG.AT-3.2 Determine if the organization provides security training when required by changes to the Smart Grid information system. SG.AT-3.3 Determine if: (i) the organization defines the frequency of refresher security-related training; and (i) the organization provides security training on an organizational defined frequency	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; security training curriculum; security training materials; security plan; training records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant Smart Grid information system security responsibilities].
SG.AT-4	Security Awareness and Training Records	SG.AT-4.1 Determine if the organization maintains training records for each user in accordance with the organization records retention policy.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security training records; security awareness and training records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security training record retention responsibilities].
SG.AT-5	Contact with Security Groups and Associations	SG.AT-5.1 Determine if: (i) the organization establishes contact with security group and associations; (ii) the organization maintains contact with security group and associations; (iii) the organization stays up to date on the latest recommended security practices, techniques, and technologies; and (iv) the organization shares current security-related information including threats, vulnerabilities, and incidents.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing Smart Grid information system security knowledge, expertise, and general information; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security responsibilities (e.g., individuals that have contacts with selected groups and associations within the security community)].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AT-6	Security Responsibility Training	SG.AT-6.1 Determine if the organization tests the knowledge of personnel on their security policies and procedures to ensure understanding of responsibilities. SG.AT-6.2 Determine if : (i) the organization maintains a list of security responsibilities for each role; and (ii) the organization tests each user in accordance with the provisions of the organization training policy. SG.AT-6.3 Determine if : (i) the organization defines the frequency to conduct security responsibility testing; and (i) the organization conducts security responsibility testing on an organizational defined frequency.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; security training plan; procedures addressing security training plan development and implementation; list of security responsibilities for each role; results of security responsibility tests; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security training responsibilities for the Smart Grid information system].
SG.AT-7	Planning Process Training	SG.AT-7.1 Determine if: (i) the organization security training includes the planning process on implementing Smart Grid information systems security plans; and (ii) the organization security training includes employees, contractors and third parties.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; Security training plan; procedures addressing security training plan development and implementation; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security training responsibilities for the Smart Grid information system].
Audit and Accountability (SG.AU-1)				
SG.AU-1	Audit and Accountability	SG.AU-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the audit and accountability security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented audit and accountability security policy that addresses— (I) the objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the audit and accountability security policy and	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with audit and accountability responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		associated audit and accountability protection requirements. SG. AU -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. AU -1.3 Determine if the organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.AU-2	Auditable Events	SG.AU-2.1 Determine if: (i) the organization develops a list of auditable events for the Smart Grid information system based on a risk assessment; and (ii) the organization defines the frequency to develop a list of auditable events. SG.AU-2.2 Determine if the organization-defined list of auditable events includes execution of privileged functions. SG.AU-2.3 Determine if the organization revises the list of auditable events based on current threat data, assessment of risk, and post-incident analysis. SG.AU-2.4 (requirements enhancement 1) Determine if the organization audits activities associated with configuration changes to the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing auditable events; security plan; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; list of organization-defined auditable events; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing information system auditing of organization-defined auditable events].
SG.AU-3	Content of Audit Records	SG.AU-3.1 Determine if: (i) the organization defines the list of events the Smart Grid information system must be capable of auditing; (ii) the Smart Grid information system produces audit records for each event; and (iii) the audit records include: (a) date and time of the event; (b) component where the event occurred; (c) type of event;	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; Smart Grid information system audit records; Smart Grid information system incident reports; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing Smart Grid information system auditing of auditable events].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(d) user/subject identity; and (e) outcome of the event.		
SG.AU-4	Audit Storage Capacity	SG.AU-4.1 Determine if: (i) the organization defines the audit record storage capacity for all Smart Grid information systems; (ii) the organization allocates audit record storage capacity in accordance with the organization-defined limits; and (iii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit storage capacity; Smart Grid information system design documentation; organization-defined audit record storage capacity for Smart Grid information system components that store audit records; list of organization-defined auditable events; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Audit record storage capacity and related configuration settings].
SG.AU-5	Response to Audit Processing Failures	SG.AU-5.1 Determine if: (i) the organization designates organizational officials to be notified in case of an audit processing failure; and (ii) the Smart Grid information system alerts designated organizational officials. SG.AU-5.2 Determine if: (i) the organization defines a set of actions to be taken in the event of an audit processing failure; and (ii) the Smart Grid information system performs the organization-defined actions when audit processing failures occur. SG.AU-5.3 (requirement enhancement 1) Determine if: (i) the organization defines the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided; and (ii) the Smart Grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity. SG.AU-5.4 (requirement enhancement 2) Determine if: (i) the organization defines audit failure events requiring real-time alerts; and (ii) the Smart Grid information system provides a real-time alert when organization-defined audit failure events occur.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing information system response to audit processing failures; automated mechanisms implementing audit storage limit warnings; automated mechanisms implementing real-time audit alerts when organization-defined failure events occur].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AU-6	Audit Monitoring, Analysis, and Reporting	SG.AU-6.1 Determine if: (i) the organization defines the frequency of Smart Grid information system audit record reviews and analysis; (ii) the organization reviews and analyzes Smart Grid information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; and (iii) the organization reports findings of inappropriate or unusual activities to the designated management authority. SG.AU-6.2 Determine if organization adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs due to organizational operations, organizational assets, or individuals.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; threat information documentation from law enforcement, intelligence community, or other sources; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities]. Test: [SELECT FROM: Smart Grid information system audit review, analysis, and reporting capability].
SG.AU-7	Audit Reduction and Report Generation	SG.AU-7.1 Determine if the Smart Grid information system provides audit reduction and report generation tools capabilities.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit reduction and report generation; Smart Grid information system design documentation; audit reduction, review, and reporting tools; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities]. Test: [SELECT FROM: Audit reduction and report generation capability].
SG.AU-8	Time Stamps	SG.AU-8.1 Determine if the Smart Grid information system uses internal system clocks to generate time stamps for audit records. SG.AU-8.2 (requirement enhancement 1) Determine if: (i) the organization defines a time source for clock synchronization; (ii) the organization defines the frequency for clock synchronization; and (iii) Smart Grid information system components synchronize internal clocks at the organization-defined frequency using an organization-defined time source.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing time stamp generation; and automated mechanisms implementing internal Smart Grid information system clock synchronization].
SG.AU-9	Protection of Audit Information	SG.AU-9.1 Determine if the Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; Smart Grid information system design documentation;

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Smart Grid information system configuration settings and associated documentation, Smart Grid information system audit records; audit tools; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing audit information protection].
SG.AU-10	Audit Record Retention	SG.AU-10.1 Determine if: (i) the organization defines the retention period for audit records generated by the Smart Grid information system; and (ii) the organization retains Smart Grid information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record retention responsibilities].
SG.AU-11	Conduct and Frequency of Audits	SG.AU-11.1 Determine if: (i) the organization defines the frequency of audits; (ii) the organization conducts audits in accordance with the organization-defined frequency; and (iii) the audits assess conformance to specified security requirements and applicable laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with audit and accountability responsibilities].
SG.AU-12	Auditor Qualification	SG.AU-12.1 Determine if the organization's audit program specifies auditor qualifications.	Examine	Examine: [SELECT FROM: Audit and accountability policy and procedures; Auditor job description/qualification document; and other relevant documents or records].
SG.AU-13	Audit Tools	SG.AU-13-1 Determine if the organization specifies the rules and conditions of use for audit tools	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit tools; Smart Grid information system design documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities].
SG.AU-14	Security Policy Compliance	SG.AU-14.1 Determine if the organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing security policy compliance; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit program responsibilities].
SG.AU-15	Audit Generation	SG.AU-15.1	Examine, Interview	Examine: [SELECT FROM: Audit and accountability

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the Smart Grid information system provides audit record generation capability for the selected list of auditable events. SG.AU-15.2 (i) Determine if the Smart Grid information system allows authorized users to select auditable events at the organization-defined Smart Grid information system components.		policy; procedures addressing audit record generation; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record generation responsibilities].
SG.AU-16	Non-Repudiation	SG.AU-16.1 Determine if the Smart Grid information system protects against an individual falsely denying having performed a particular action.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing non-repudiation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing non-repudiation capability].
Security Assessment and Authorization (SG.CA)				
SG.CA-1	Security Assessment and Authorization Policy and Procedures	SG.CA-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the security assessment and authorization security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented security assessment and authorization security policy that addresses— (I) the objectives, roles, and responsibilities for the security assessment and authorization security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the security assessment and authorization security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the security assessment and authorization security policy and associated security assessment and authorization protection requirements. SG. CA -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policies and procedures; other relevant documents or records; and applicable federal, state, local, tribal, and territorial laws and regulations]. Interview: [SELECT FROM: Organizational personnel with specific security assessment and authorization responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. CA -1.3 Determine if the organization ensures that the security assessment and authorization security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CA-2	Security Assessments	SG.CA-2.1 Determine if the organization develops a security assessment plan for the Smart Grid IT system that describes the scope of the assessment including— (i) security requirements and requirement enhancements under assessment; (ii) assessment procedures to be used to determine security requirement effectiveness; and (iii) assessment environment, assessment team, and assessment roles and responsibilities. SG.CA-2.2 Determine if : (i) the organization defines the frequency of assessing the security requirements in the Smart Grid information system; and (ii) the organizations assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are: (a) implemented correctly; (b) operating as intended; and (c) producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system. SG.CA-2.3 Determine if the organization produces a security assessment report that documents the results of the assessment. SG.CA-2.4 Determine if the organization provides the results of the security requirements assessment to a management authority.	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security assessment responsibilities].
SG.CA-3	Continuous Improvement	SG.CA-3.1 Determine if: (i) the organization's security program defines a continuous improvement practices process for the Smart Grid	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessments and policies; security policies; security plan; security assessment plan; security assessment

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		information system security policies and procedures; (ii) the organization defines relevant industry lessons learned and best practices for Smart Grid information system security policies and procedures; and (iii) the continuous improvement process incorporates industry lessons learned and best practices into Smart Grid information system security policy and procedures.		report; security assessment evidence; plan of action and milestones; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security assessment responsibilities; organizational personnel with security management responsibilities; and organizational personnel with security policy and procedure development.
SG.CA-4	Information System Connections	SG.CA-4.1 Determine if: (i) the organization authorizes all connections from the Smart Grid information system to other Smart Grid information systems; (ii) the organization identifies connections from Smart Grid information system to external information systems; and (iii) the organization authorizes connections from the Smart Grid information system to external information systems. SG.CA-4.2 Determine if the organization documents the Smart Grid information system connections and associated security requirements for each connection. SG.CA-4.3 Determine if the organization monitors the Smart Grid information system connections on an ongoing basis to verify enforcement of documented security requirements.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing Smart Grid information system connections; system and communications protection policy; Smart Grid information system interconnection security agreements; security plan; Smart Grid information system design documentation; security assessment report; plan of action and milestones; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibility for developing, and implementing, or approving Smart Grid information system interconnection agreements].
SG.CA-5	Security Authorization to Operate	SG.CA-5.1 Determine if: (i) the organization authorizes the Smart Grid information system for processing before operation; (ii) the organization updates authorization based on an organization-defined frequency, or when a significant change occurs to the Smart Grid information system; (iii) the organization defines the frequency of updates to the authorization; and (iv) the organization updates the authorization in accordance with an organization-defined frequency. SG.CA-5.2 Determine if: (i) the organization documents a management authority to sign and approve the security authorization to operate; (ii) the documented management authority signs and approves the security authorization to operate; (iii) the organization conducts and reviews security	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security authorization responsibilities for Smart Grid information systems].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		assessments in support of security authorizations on an organization-defined frequency; and (iv) the organization defines the frequency to conduct and review security assessments in support of security authorizations.		
SG.CA-6	Continuous Monitoring	SG.CA-6.1 Determine if the organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy. SG.CA-6.2 Determine if the organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: (i) reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency; (ii) the organization documents the management authority receiving the security state reports of the Smart Grid information system; and the organization defines the organizational frequency for reporting the security state of the Smart Grid information system to the management authority.	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing continuous monitoring of Smart Grid information system security controls; security plan; security assessment report; plan of action and milestones; Smart Grid information system monitoring records; status reports; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with continuous monitoring responsibilities].
Configuration Management (SG.CM)				
SG.CM-1	Configuration Management Policy and Procedures	SG.CM-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the configuration management security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented configuration management security policy that addresses— (I) the objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements.	Examine, Interview	Examine: [SELECT FROM: Configuration management policies and procedures; other relevant documents or records; and applicable federal, state, local, tribal, and territorial laws and regulations]. Interview: [SELECT FROM: Organizational personnel with configuration management and control responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG. CM -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. CM -1.3 Determine if the organization ensures that the configuration management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CM-2	Baseline Configuration	SG.CM-2.1 Determine if: (i) the organization (a) develops the current baseline configuration of the Smart Grid information system; (b) documents the current baseline configuration of the Smart Grid information system; and (c) maintains the current baseline configuration of the Smart Grid information system; (ii) the organization maintains an inventory of the Smart Grid information system's constituent components; (iii) the organization reviews the baseline configuration as an integral part of Smart Grid information system component installations; and (iv) the organization updates the baseline configuration as an integral part of Smart Grid information system component installations.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the Smart Grid information system; Smart Grid information system architecture documentation; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with configuration change control responsibilities].
SG.CM-3	Configuration Change Control	SG.CM-3.1 Determine if: (i) the organization documents changes to the Smart Grid information system; and (ii) the organization authorizes changes to the Smart Grid information system. SG.CM-3.2 Determine if: (i) the organization retains records of configuration-managed changes to the Smart Grid information system; and (ii) the organization reviews records of configuration-managed changes to the Smart Grid information system on an organizational defined frequency.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing Smart Grid information system configuration change control; Smart Grid information system architecture and configuration documentation; automated configuration control mechanisms; change control records; Smart Grid information system audit records; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with configuration change control responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.CM-3.3 Determine if the organization audits activities associated with configuration-managed changes to the Smart Grid information system. SG.CM-3.4 Determine if: (i) the organization tests configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system; (ii) the organization validates configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system; and (iii) the organization documents configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system.		
SG.CM-4	Monitoring Configuration Changes	SG.CM-4.1 Determine if: (i) the organization documents a process to monitor changes to the Smart Grid information system; and (ii) the organization implements a process to monitor changes to the Smart Grid information system. SG.CM-4.2 Determine if the organization, prior to change implementation and as part of the change approval process, analyzes changes to the Smart Grid information system for potential security impacts. SG.CM-4.3 Determine if the organization, after the Smart Grid information system is changed, checks the security features to ensure that the features are still functioning properly.	Examine, Interview	Examine: [SELECT FROM: configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the Smart Grid information system; security impact analysis documentation; Smart Grid information system architecture and configuration documentation; change control records; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for determining security impacts prior to implementation of Smart Grid information system changes].
SG.CM-5	Access Restrictions for Configuration Change	SG.CM-5.1 Determine if: (i) the organization defines individual access privileges associated with configuration changes to the Smart Grid information system; (ii) the organization documents individual access privileges associated with configuration changes to the Smart Grid information system; (iii) the organization approves individual access privileges associated with configuration changes to the Smart Grid information system; and (iv) the organization enforces access restrictions associated with configuration changes to the Smart Grid information	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the Smart Grid information system; list software programs that meet the terms and conditions for installation on Smart Grid information devices; Smart Grid information system design documentation; security plan; Smart Grid information system architecture and configuration documentation; change control records; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		system. SG.CM-5.2 Determine if: (i) the organization generates records reflecting changes to individual access privileges on the Smart Grid information system; (ii) the organization retains records reflecting changes to individual access privileges on the Smart Grid information system; and (iii) the organization reviews records reflecting changes to individual access privileges on the Smart Grid information system. SG.CM-5.3 Determine if the organization establishes terms and conditions for installing any hardware, firmware, or software on Smart Grid information system devices. SG.CM-5.4 Determine if: (i) the organization defines the frequency for conducting audits of Smart Grid information system changes; and (ii) the organization conducts audits of Smart Grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred.		with logical access control responsibilities; and organizational personnel with physical access control responsibilities]. Test: [SELECT FROM: Change control process and associated restrictions for changes to the Smart Grid information system; Smart Grid information system mechanisms preventing installation of software programs not meeting the terms and conditions for installation; and Smart Grid information system implementing safeguards and countermeasures for inappropriate changes to security functions].
SG.CM-6	Configuration Settings	SG.CM-6.1 Determine if the organization establishes configuration settings for components within the Smart Grid information system. SG.CM-6.2 Determine if: (i) the organization monitors changes to the configuration settings in accordance with organizational policies and procedures; and (ii) the organization controls changes to the configuration settings in accordance with organizational policies and procedures. SG.CM-6.3 Determine if the organization documents changed configuration settings. SG.CM-6.4 Determine if:	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing configuration settings for the Smart Grid information system; security plan; Smart Grid information system configuration settings and associated documentation; security configuration checklists; Smart Grid information system design documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security configuration responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization identifies exceptions from the configuration settings in accordance with organizational policies and procedures; (ii) the organization documents exceptions from the configuration settings in accordance with organizational policies and procedures; and (iii) the organization approves exceptions from the configuration settings in accordance with organizational policies and procedures. SG.CM-6.5 Determine if the organization enforces the configuration settings in all components of the Smart Grid information system.		
SG.CM-7	Configuration for Least Functionality	SG.CM-7.1 Determine if : (i) the organization defines for the Smart Grid information system a "prohibited and/or restricted" list of functions, ports, protocols, and/or services; (ii) the organization configures the Smart Grid information system to provide only essential capabilities; and (iii) the organization configures the Smart Grid information system to specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list. SG.CM-7.2 Determine if : (i) the organization defines the frequency of information system reviews to identify and eliminate unnecessary functions, ports, protocols, and/or services; and (ii) the organization reviews the Smart Grid information system on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services.	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing least functionality in the Smart Grid information system; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the Smart Grid information system]. Test: [SELECT FROM: Smart Grid information system for disabling or restricting functions, ports, protocols, and services].
SG.CM-8	Component Inventory	SG.CM-8.1 Determine if the organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that accurately reflects the current Smart Grid information system configuration. SG.CM-8.2 Determine if the organization provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; Smart Grid information system design documentation; procedures addressing Smart Grid information system component inventory; security plan; Smart Grid information system inventory records; component installation records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for defining Smart Grid

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.CM-8.3 Determine if the organization identifies the roles responsible for component inventory. SG.CM-8.4 Determine if the organization updates the inventory of system components as an integral part of component installations, system updates, and removals. SG.CM-8.5 Determine if the organization ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary.		information system components within the authorization boundary of the system; and organizational personnel with Smart Grid information system installation and inventory responsibilities].
SG.CM-9	Addition, Removal, and Disposal of Equipment	SG.CM-9.1 Determine if the organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment. SG.CM-9.2 Determine if all Smart Grid information system components and information are documented, identified, and tracked so that their location and function are known.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; Smart Grid information system design documentation; procedures addressing Smart Grid information system component inventory; security plan; Smart Grid information system inventory records; Smart Grid information system inventory records; component installation records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system installation and inventory responsibilities; and organizational personnel with configuration management responsibilities].
SG.CM-10	Factory Default Settings Management	SG.CM-10.1 Determine if the organization policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on Smart Grid information system components and applications. SG.CM-10.2 Determine if: (i) the organization changes the factory default settings upon installation; and (ii) the organization changes the factory default settings if used during maintenance.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing configuration settings for the Smart Grid information system; configuration standard documents; procedures addressing configuration management planning; security plan; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for configuration management process development; organizational personnel with configuration management responsibilities; and organizational personnel with Smart Grid information system installation and maintenance responsibilities].
SG.CM-11	Configuration Management Plan	SG.CM-11.1 Determine if the organization develops and implements a configuration management plan for the Smart Grid	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing responsibilities for configuration

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		information system that addresses roles, responsibilities, and configuration management processes and procedures. SG.CM-11.2 Determine if the organization defines the configuration items for the Smart Grid information system. SG.CM-11.3 Determine if the organization defines when (in the system development life cycle) the configuration items are placed under configuration management. SG.CM-11.4 Determine if the organization defines the means for uniquely identifying configuration items throughout the system development life cycle. SG.CM-11.5 Determine if the organization defines the process for managing the configuration of the controlled items.		management process development; procedures addressing configuration management planning; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for configuration management process development].
Continuity of Operations (SG.CP)				
SG.CP-1	Continuity of Operations Policy and Procedures	SG.CP-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the continuity of operations security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented continuity of operations security policy that addresses— (I) the objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the continuity of operations security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements. SG. CP -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security	Examine, Interview	Examine: [SELECT FROM: Continuity of operations policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with continuity of operations responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. CP -1.3 Determine if the organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CP-2	Continuity of Operations Plan	SG.CP-2.1 Determine if: (i) the organization develops a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system; (ii) the organization documents a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system; and (iii) the organization implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system. SG.CP-2.2 Determine if the organizational continuity of operations plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring Smart Grid information system operations after a disruption or failure. SG.CP-2.3 Determine if: (i) the organization document a management authority for the continuity of operations plan; and (ii) the management authority reviews and approves the continuity of operations plan.	Examine, Interview	Examine: [SELECT FROM: Continuity of operations policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with continuity of operations responsibilities].
SG.CP-3	Continuity of Operations Roles and Responsibilities	SG.CP-3.1 Determine if the organizational continuity of operations plan for Smart Grid information systems defines the roles and responsibilities of the various employees and contractors in the event of a significant incident. SG.CP-3.2 Determine if the organization identifies responsible personnel to lead the recovery and response effort if an incident occurs.	Examine, Interview	Examine: [SELECT FROM: Continuity of operations policy; procedures addressing continuity of operations for the Smart Grid information system; continuity of operations plan; security plan; business impact assessment; other related plans; alternate processing site agreements; alternate storage site agreements; continuity of operations plan testing and/or exercise documentation; continuity of operations plan test results; and other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Interview: [SELECT FROM: Organizational personnel with continuity of operations planning/plan implementation responsibilities and responsibilities in related plan areas].
SG.CP-4	Continuity of Operations Training	SG.CP-4.1 Determine if: (i) the organization trains personnel in their continuity of operations roles and responsibilities with respect to the Smart Grid information system; and (ii) the organization provides refresher training to personnel on their continuity of operations roles and responsibilities on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Continuity of operations policy; continuity of operations plan; procedures addressing continuity of operations training; continuity of operations training curriculum; continuity of operations training material; security plan; continuity of operations training records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with continuity of operations planning, plan implementation, and training responsibilities].
SG.CP-5	Continuity of Operations Plan Testing	SG.CP-5.1 Determine if: (i) the continuity of operations plan is tested to determine its effectiveness; and (ii) the continuity of operations plan testing results are documented. SG.CP-5.2 Determine if: (i) the organization documented a management authority to review continuity of operations plan test results; and (ii) the management authority reviews the documented test results and initiates corrective actions, if necessary. SG.CP-5.3 Determine if: (i) the organization defines tests for the continuity of operations plan for the Smart Grid information systems; and (ii) the organization tests the continuity of operations plan for the Smart Grid information system on an organization-defined frequency. SG.CP-5.4 (requirement enhancements 1) Determine if the organization coordinates continuity of operations plan testing and exercises with all affected organizational elements.	Examine, Interview	Examine: [SELECT FROM: Continuity of operations policy; Continuity of operations plan, procedures addressing continuity of operations plan testing and exercises; security plan; continuity of operations plan testing and/or exercise documentation; continuity of operations plan test results; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing or responding to continuity of operations plan tests/exercises; organizational personnel with Smart Grid information system recovery and reconstitution responsibilities; organizational personnel with continuity of operations plan testing and/or exercise responsibilities; organizational personnel with continuity of operations planning, plan implementation, and testing responsibilities; and organizational personnel with responsibilities for related plans].
SG.CP-6	Continuity of Operations Plan Update	SG.CP-6.1 Determine if: (i) the organization reviews the continuity of operations plan for the Smart Grid information system on an	Examine, Interview	Examine: [SELECT FROM: Continuity of operations policy; procedures addressing continuity of operations for the Smart Grid information system; continuity of operations plan; security plan; business impact

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		organizational defined frequency; and (ii) the organization updates the continuity of operations plan on an organization-defined frequency to address Smart Grid information system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.		assessment; other related plans; alternate processing site agreements; alternate storage site agreements; continuity of operations plan testing and/or exercise documentation; continuity of operations plan test results; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with continuity of operations planning and plan implementation responsibilities and responsibilities in related plan areas; and organizational personnel with incident handling responsibilities].
SG.CP-7	Alternate Storage Sites	SG.CP-7.1 Determine if: (i) the organization determines the requirement for an alternate storage site for continuity of operations; and (ii) the organization initiates any necessary agreements for an alternate storage site for continuity of operations. SG.CP-7.2 (requirement enhancements 1) Determine if the organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. SG.CP-7.3 (requirement enhancements 2) Determine if the organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards. SG.CP-7.4 (requirement enhancements 3) Determine if the organization configures the alternate storage site to facilitate timely and effective recovery operations.	Examine	Examine: [SELECT FROM: Continuity of operations policy; continuity of operations plan; procedures addressing alternate storage sites; alternate storage site; alternate storage site agreements; mitigation actions for accessibility problems to the alternate storage site; and other relevant documents or records].
SG.CP-8	Alternate Telecommunication Services	SG.CP-8.1 Determine if: (i) the organization identifies alternate telecommunication services for the Smart Grid information system for continuity of operations; and (ii) the organization initiates necessary agreements to permit the resumption of operations for the safe operation of the Smart Grid information system within an organization-defined time period when the primary Smart Grid information system capabilities are unavailable. SG.CP-8.2 (requirement enhancement 1) Determine if: (i) primary telecommunication service agreements contain	Examine, Interview	Examine: [SELECT FROM: Continuity of Operations policy; continuity of operations plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; list of essential missions and business functions; primary telecommunications service provider's site; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with planning, plan implementation, and testing responsibilities; and telecommunications service providers].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		priority-of-service provisions in accordance with the organization's availability requirements; and (ii) alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements. SG.CP-8.3 (requirement enhancement 2) Determine if alternate telecommunication services do not share a single point of failure with primary telecommunication services. SG.CP-8.4 (requirement enhancement 3) Determine if alternate telecommunication service providers are sufficiently separated from primary service providers so they are not susceptible to the same hazards. SG.CP-8.5 (requirement enhancement 4) Determine if: (i) primary telecommunication service providers have adequate contingency plans; and (ii) alternate telecommunication service providers have adequate contingency plans.		
SG.CP-9	Alternate Control Center	SG.CP-9.1 Determine if: (i) the organization defines critical functions; (ii) the organization identifies an alternate control center and necessary telecommunications to permit the resumption of Smart Grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable; and (iii) the organization initiates any necessary agreements to permit the resumption of Smart Grid information system operations for critical functions when the primary control center is unavailable. SG.CP-9.2 (requirement enhancements 1) Determine if the organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards. SG.CP-9.3 (requirement enhancements 2) Determine if: (i) the organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster; and (ii) the organization outlines explicit mitigation actions for	Examine	Examine: [SELECT FROM: Continuity of operations policy; continuity of operations plan; procedures addressing an alternate control center; alternate control center agreements; service level agreements; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; list of critical functions; alternate control center; and other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		potential accessibility problems for the alternate control center. SG.CP-9.4 (requirement enhancements 3) Determine if the organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.		
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	SG.CP-10.1 Determine if: (i) the organization provides the capability to recover and reconstitute the Smart Grid information system to a known secure state after a disruption, compromise, or failure; and (ii) the organization documents the Smart Grid information system known, secure state. SG.CP-10.2 (requirement enhancement 1) Determine if: (i) the organization defines in the security plan, the circumstances that can inhibit recovery and reconstitution of the Smart Grid information system to a known, secure state; and (ii) the organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state. SG.CP-10.3 (requirement enhancement 2) Determine if: (i) the organization defines the time-periods within which the Smart Grid information system components must be reimaged from configuration-controlled and integrity-protected media images representing a secure, operational state for the components; and (ii) the organization provides the capability to reimage Smart Grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components.	Examine, Interview, Test	Examine: [SELECT FROM: Continuity of operations policy; continuity of operations plan; procedures addressing Smart Grid information system recovery and reconstitution; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; continuity of operations plan test procedures; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities]. Test: [SELECT FROM: Automated mechanisms and/or manual procedures for implementing Smart Grid information system recovery and reconstitution operations].
SG.CP-11	Fail-Safe Response	SG.CP-11.1 Determine if the Smart Grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart Grid information systems or the loss of the Smart Grid information system itself.	Examine, Interview, Test	Examine: [SELECT FROM: Continuity of operations policy; plan; procedures addressing Smart Grid information system recovery and reconstitution; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; security

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities]. Test: [SELECT FROM: Automated mechanisms and/or manual procedures for implementing Smart Grid information system recovery and reconstitution operations].
Identification and Authentication (SG.IA)				
SG.IA-1	Identification and Authentication Policy and Procedures	SG.IA-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the identification and authentication security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented identification and authentication security policy that addresses— (I) the objectives, roles, and responsibilities for the identification and authentication security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the identification and authentication security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements. SG. IA -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. IA -1.3 Determine if the organization ensures that the identification and authentication security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Identification and authentication policy and procedures; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with identification and authentication responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.IA-2	Identifier Management	SG.IA-2.1 Determine if the organization received authorization from a management authority to assign a user or device identifier.	Examine, Interview	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of Smart Grid information system accounts; list of identifiers generated from physical access control devices; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with identifier management responsibilities].
SG.IA-3	Authenticator Management	SG-IA-3.1 Determine if the organization manages the Smart Grid information system authentication credential for users and devices by defining initial authentication credential content, such as defining password length and composition, tokens for authentication defined by the organization. SG-IA-3.2 Determine if the organization establishing administrative procedures for: (i) initial authentication credential distribution; (ii) lost, compromised, or damaged authentication credentials; and (iii) revoking authentication credentials. SG-IA-3.3 Determine if the organization defines the frequency for authentication credential changing/refreshing. SG-IA-3.4 Determine if the organization specifies measures to safeguard authentication credentials.	Examine, Interview, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content]. Test: [SELECT FROM: Automated mechanisms implementing authenticator management functions].
SG.IA-4	User Identification and Authentication	SG.IA-4.1 Determine if: (i) the Smart Grid information system uniquely identifies users or processes acting on behalf of users; and (ii) the Smart Grid information system authenticates users or processes acting on behalf of users.	Examine, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; list of Smart Grid information system accounts; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing identification and authentication

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				capability for the Smart Grid information system].
SG.IA-5	Device Identification and Authentication	SG.IA-5.1 Determine if the organization defines the list of devices for which identification and authentication is required before establishing a connection to the Smart Grid information system. SG.IA-5.2 (requirement enhancement 1) Determine if the Smart Grid information system uniquely identified an organization-defined device before establishing a connection. SG.IA-5.2 (requirement enhancement 2) Determine if the Smart Grid information system authenticates an organization-defined device before establishing a connection.	Examine	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing device identification and authentication; Smart Grid information system design documentation; list of devices requiring unique identification and authentication; device connection reports; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records].
SG.IA-6	Authenticator Feedback	SG.IA-6.1 Determine if the organization authentication mechanisms in the Smart Grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Examine, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing authenticator feedback; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing authenticator feedback].
Identification and Document Management (SG.ID)				
SG.ID-1	Information and Document Management Policy and Procedures	SG.ID-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the information and document management security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented information and document management security policy that addresses— (I) the objectives, roles, and responsibilities for the information and document management security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the information and document management security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the information and document management security policy and associated information and document	Examine, Interview	Examine: [SELECT FROM: Information and document management policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with information and document management responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		management protection requirements. SG. ID -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. ID -1.3 Determine if the organization ensures that the information and document management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.ID-2	Information and Document Retention	SG.ID-2.1 Determine if the organization develops policies and procedures detailing the retention of organization information. SG.ID-2.2 Determine if the organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations. SG.ID-2.3 Determine if the organization manages Smart Grid information system-related data including establishing retention policies and procedures for both electronic and paper data. SG.ID-2.4 Determine if the organization manages access to Smart Grid information system-related data based on assigned roles and responsibilities.	Examine, Interview	Examine: [SELECT FROM: Information and document management policy and procedures; retention policies and procedures for electronic and paper data; Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; Smart Grid information system audit records System and information integrity policy; procedures addressing Smart Grid information system output handling and retention; media protection policy and procedures; information retention records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with information and document management responsibilities; organizational personnel with Smart Grid information system audit record retention responsibilities; and organizational personnel with information output handling and retention responsibilities].
SG.ID-3	Information Handling	SG.ID-3.1 Determine if: (i) the organization-implemented policies and procedures detailing the handling of information are developed; and (ii) the organization-implemented policies and procedures detailing the handling of information are reviewed on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Information and document management policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with information and document management responsibilities].
SG.ID-4	Information Exchange	SG.ID-4.1 Determine if the organization establishes agreements for the exchange of information, firmware, and software between the organization and external parties such as third parties,	Examine, Interview	Examine: [SELECT FROM: Information and document management policy and procedures; information exchange agreements; Smart Grid information system design documentation; Smart Grid information system

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		vendors and contractors.		configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with responsibility for interfacing with external parties (third parties, vendors, contractors)].
SG.ID-5	Automated Labeling	SG.ID-5.1 Determine if the Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with access control requirements. SG.ID-5.2 Determine if the Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with special dissemination, handling, or distribution instructions. SG.ID-5.3 Determine if the Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance as required by the Smart Grid information system security policy.	Examine, Test	Examine: [SELECT FROM: Information and document management policy and procedures; access control policy and procedures; Smart Grid information system labeling policy; procedures addressing information labeling; security plan; storage media and Smart Grid information system output; and other relevant documents or records]. Test: [Automated mechanisms implementing automatic labeling of information].
Incident Response (SG.IR)				
SG.IR-1	Incident Response Policy and Procedures	SG.IR-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the incident response security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented incident response security policy that addresses— (I) the objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the incident response security policy and associated incident response protection requirements. SG. IR -1.2 Determine if: (i) the organization documents management commitment	Examine, Interview	Examine: [SELECT FROM: Incident response policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response and responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. IR -1.3 Determine if the organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.IR-2	Incident Response Roles and Responsibilities	SG.IR-2.1 Determine if the organization's Smart Grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents. SG.IR-2.2 Determine if: (i) the plan identifies responsible personnel to lead the response effort if an incident occurs; and (ii) the organization identifies response teams to reestablish operations that include Smart Grid information system and other process owners.	Examine, Interview	Examine: [SELECT FROM: Incident response policy and procedures; system security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response responsibilities].
SG.IR-3	Incident Response Training	SG.IR-3.1 Determine if: (i) personnel are trained on an organization-defined frequency in their incident response roles and responsibilities with respect to the Smart Grid information system ; (ii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; (iii) the organization defines the frequency of refresher incident response training; and (iv) personnel receive refresher training on an organization-defined frequency for their incident response roles and responsibilities.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response training and operational responsibilities].
SG.IR-4	Incident Response Testing and Exercises	SG.IR-4.1 Determine if: (i) the organization defines incident response test/exercises; (ii) the organization defines the frequency of incident response tests/exercises; (iii) the organization tests and/or exercises the incident response capability for the Smart Grid information system at an organization-defined frequency using	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing documentation; incident response plan; incident response testing material; incident response test results; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response testing responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results; (iv) the organization documents the test and/or exercise results on the incident response capability for the Smart Grid information system; and (v) the organization determines the effectiveness of the incident response capability.		
SG.IR-5	Incident Handling	SG.IR-5.1 Determine if the organization implements an incident handling capability for security incidents that includes: (i) preparation (ii) detection (iii) analysis (iv) containment (v) mitigation; and (vi) recovery. SG.IR-5.2 Determine if the organization integrates incident handling procedures with continuity of operations procedures. SG.IR-5.3 Determine if the organization incorporates lessons learned from incident handling activities into incident response procedures.	Examine, Interview, Test	Examine: [SELECT FROM: Incident response policy; procedures addressing incident handling; incident response plan; security plan; incident response plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident handling responsibilities; and organizational personnel with continuity of operations responsibilities]. Test: [SELECT FROM: Incident handling capability for the organization].
SG.IR-6	Incident Monitoring	SG.IR-6.1 Determine if: (i) the organization tracks Smart Grid information system and network security incidents; and (ii) the organization documents Smart Grid information system and network security incidents.	Examine, Interview, Test	Examine: [SELECT FROM: Incident response policy; procedures addressing incident monitoring; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; incident response records and documentation; automated mechanisms supporting incident monitoring; incident response plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident monitoring responsibilities]. Test: [SELECT FROM: Incident monitoring capability for the organization; and Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information].
SG.IR-7	Incident Reporting	SG.IR-7.1 Determine if the organization incident reporting procedure includes: (i) What is a reportable incident; (ii) The granularity of the information reported;	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; automated mechanisms supporting incident reporting; and other relevant

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(iii) Who receives the report; and (iv) The process for transmitting the incident information. SG.IR-7.2 Determine if the organization's detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations.		documents or records]. Interview: [SELECT FROM: Organizational personnel with incident reporting responsibilities].
SG.IR-8	Incident Response Investigation and Analysis	SG.IR-8.1 Determine if the organization policies and procedures include an incident response investigation and analysis program. SG.IR-8.2 Determine if the organization includes investigation and analysis of Smart Grid information system incidents in the planning process. SG.IR-8.3 Determine if: (i) the organization develops an incident investigation and analysis process; (ii) the organization tests an incident investigation and analysis process; (iii) the organization deploys an incident investigation and analysis process; and (iv) the organization documents an incident investigation and analysis process.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident investigation and analysis; incident investigation and analysis processes; incident investigation and analysis processes test plans and results; Smart Grid information system design documentation; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response investigation and analysis responsibilities].
SG.IR-9	Corrective Action	SG.IR-9.1 Determine if the organization reviews investigation results and determines corrective actions needed. SG.IR-9.2 Determine if the organization includes processes and mechanisms in the planning to ensure that corrective actions identified.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response and corrective actions; incident response planning processes; Smart Grid information system design documentation; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident investigation and corrective action].
SG.IR-10	Smart Grid Information System Backup	SG.IR-10.1 Determine if: (i) the organization defines the frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives; and (ii) the organization conducts backups of user-level information contained in the Smart Grid information system on an organization-defined frequency. SG.IR-10.2 Determine if: (i) the organization defines the frequency of conducting	Examine, Interview	Examine: [SELECT FROM: Incident response policy; incident response plan; procedures addressing Smart Grid information system backup; Smart Grid information system backup test results; incident response plan test results; incident response plan and/or exercise documentation; backup storage location(s); secondary backup storage location(s); redundant secondary system for Smart Grid information system backups; security plan alternate site service agreements; backup storage location(s); Smart Grid information system design documentation; Smart Grid information system backup logs or

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		system-level information backups to support recovery time and recovery point objectives; and (ii) the organization conducts backups of Smart Grid information system-level information (including Smart Grid information system state information) contained in the Smart Grid information system on an organization-defined frequency. SG.IR-10.3 Determine if: (i) the organization defines the frequency of conducting information system documentation backups (including security-related information) to support recovery time and recovery point objectives; and (ii) the organization conducts backups of Smart Grid information system documentation including security-related documentation on an organization-defined frequency. SG.IR-10.4 Determine if the organization protects the confidentiality and integrity of backup information at the storage location. SG.IR-10.5 (requirement enhancements 1) Determine if: (i) the organization defines the frequency of information system backup testing; and (ii) the organization tests backup information at an organization-defined frequency to verify media reliability and information integrity. SG.IR-10.6 (requirement enhancements 2) Determine if the organization selectively uses backup information in the restoration of Smart Grid information system functions as part of continuity of operations testing. SG.IR-10.7 (requirement enhancements 3) Determine if the organization stores backup copies of the operating system and other critical Smart Grid information system software in a separate facility or in a fire-rated container that is not collocated with the operational software..		records; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response planning and plan implementation responsibilities; and organizational personnel with Smart Grid information system backup responsibilities].
SG.IR-11	Coordination of Emergency Response	SG.IR-11.1 Determine if: (i) the organization's security policies and procedures delineate how the organization implements its emergency response plan; and (ii) the organization's security policies and procedures to	Examine, Interview	Examine: [SELECT FROM: Incident response/emergency management policy; procedures addressing incident response planning; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		coordinate efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.		with incident response planning responsibilities].
Smart Grid Information System Maintenance (SG.MA)				
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	SG.MA-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the Smart Grid information system maintenance security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented Smart Grid information system maintenance security policy that addresses— (I) the objectives, roles, and responsibilities for the Smart Grid information system maintenance security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the Smart Grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the Smart Grid information system maintenance security policy and associated Smart Grid information system maintenance protection requirements. SG. MA -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. MA -1.3 Determine if the organization ensures that the Smart Grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Smart Grid Information System maintenance policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities].
SG.MA-2	Legacy Smart Grid Information System Updates	SG.MA-2.1 Determine if: (i) the organization develops policies and procedures to upgrade existing legacy Smart Grid information systems; and	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing upgrades to legacy Smart Grid information systems; documentation of mitigating security measures; and other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the policies and procedures include mitigating security measures commensurate with the organization's risk tolerance and the risk to the Smart Grid information system.		Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities; organizational personnel with Smart Grid information system maintenance responsibilities; organizational personnel with legacy Smart Grid information system responsibilities].
SG.MA-3	Smart Grid Information System Maintenance	SG.MA-3.1 Determine if: (i) the organization schedules maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (ii) the organization performs maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (iii) the organization documents maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; and (iv) the organization reviews records of maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements. SG.MA-3.2 Determine if the organization explicitly approves the removal of the Smart Grid information system or Smart Grid information system components from organizational facilities for off-site maintenance or repairs. SG.MA-3.3 Determine if the organization sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. SG.MA-3.4 Determine if the organization checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions. SG.MA-3.5 Determine if the organization makes and secures backups of critical Smart Grid information system software, applications, and data for use if the operating system becomes corrupted or	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing controlled maintenance for the Smart Grid information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; maintenance records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		destroyed. SG.MA-3.6 (requirement enhancement 1) Determine if the organization maintains maintenance records for the Smart Grid information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).		
SG.MA-4	Maintenance Tools	SG.MA-4.1 Determine if: (i) the organization approves the use of Smart Grid information system maintenance tools; and (ii) the organization monitors the use of Smart Grid information system maintenance tools.	Examine	Examine: [SELECT FROM: Smart Grid information system maintenance policy; Smart Grid information system maintenance tools and associated documentation; procedures addressing Smart Grid information system maintenance tools; Smart Grid information system design documentation; maintenance records; and other relevant documents or records].
SG.MA-5	Maintenance Personnel	SG.MA-5.1 Determine if the organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the Smart Grid information system. SG.MA-5.2 Determine if authorized organizational personnel with appropriate maintenance access supervise unauthorized maintenance personnel during the performance of maintenance activities on the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities].
SG.MA-6	Remote Maintenance	SG.MA-6.1 Determine if the organization policy and procedures for remote maintenance include authorization and monitoring the use of remote maintenance and diagnostic activities. SG.MA-6.2 Determine if the organization policy and procedures for remote maintenance include use of remote maintenance and diagnostic tools. SG.MA-6.3 Determine if the organization policy and procedures for remote maintenance include maintenance records for remote maintenance and diagnostic activities. SG.MA-6.4	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing remote maintenance for the Smart Grid information system; service provider contracts and/or service level agreements; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; maintenance records; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities; and Smart Grid information system maintenance provider].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the organization policy and procedures for remote maintenance include termination of all remote maintenance sessions. SG.MA-6.5 Determine if the organization policy and procedures for remote maintenance include management of authorization credentials used during remote maintenance. SG.MA-6.6 (requirement enhancement 1) Determine if the organization requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced. SG.MA-6.7 (requirement enhancement 2) Determine if: (i) the organization removes the component to be serviced from the Smart Grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities; and (ii) the organization, after the removed component service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the Smart Grid information system.		
SG.MA-7	Timely Maintenance	SG.MA-7.1 Determine if: (i) the organization defines security-critical Smart Grid information system components for which it will obtain maintenance support and spare parts; (ii) the organization obtains maintenance support for an organization-defined list of security-critical Smart Grid information system components; and (iii) the organization obtains spare parts for an organization-defined list of security-critical Smart Grid information system components.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing timely maintenance for the Smart Grid information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities].
Media Protection (SG.MP)				
SG.MP-1	Media Protection Policy and Procedures	SG.MP-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the media protection security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented media protection security policy that	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media protection; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		addresses— (I) the objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the media protection security policy and associated media protection requirements. SG. MP -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. MP -1.3 Determine if the organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.MP-2	Media Sensitivity Level	SG.MP-2.1 Determine if: (i) the organization documents the sensitivity levels of media; and (ii) the sensitivity level of media indicates the protection required commensurate with the impact of compromise.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing security categorization of media; security planning policy and procedures; security plan; security categorization documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with media sensitivity level classification responsibilities].
SG.MP-3	Media Marking	SG.MP-3.1 Determine if: (i) the organization marks removable Smart Grid information system media in accordance with organization-defined policy and procedures; and (ii) the organization marks Smart Grid information system output in accordance with organization-defined policy and procedures.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and Smart Grid information system output; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				and marking responsibilities].
SG.MP-4	Media Storage	SG.MP-4.1 Determine if: (i) the organization documents the storage requirements of stored media based on the sensitivity of the material; (ii) the organization physically manages Smart Grid information system media within protected areas; and (iii) the organization physically stores Smart Grid information system media within protected areas.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; security plan; Smart Grid information system media; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection and storage responsibilities].
SG.MP-5	Media Transport	SG.MP-5.1 Determine if: (i) the organization defines types of media protected during transport outside of controlled areas and security measures (e.g., locked container, encryption) for such media transported outside of controlled areas; and (ii) the organization protects organization-defined types of media during transport outside controlled areas using organization-defined security measures. SG.MP-5.2 Determine if the organization maintains accountability for Smart Grid information system media during transport outside controlled areas. SG.MP-5.3 Determine if the organization restricts the activities associated with transport of Smart Grid information system media to authorized personnel.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport Smart Grid information system media outside of controlled areas; Smart Grid information system media; Smart Grid information system media transport records; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media transport responsibilities].
SG.MP-6	Media Sanitization and Disposal	SG.MP-6.1 Determine if: (i) the organization sanitizes Smart Grid information system media before disposal or release for reuse; (ii) the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance; and (iii) the organization tests sanitization equipment and procedures to verify correct performance on an organization-defined frequency. SG.MP-6.2 (requirement enhancement 1) Determine if:	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; media sanitization equipment test records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media sanitization responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization tracks media sanitization and disposal actions; (ii) the organization documents media sanitization and disposal actions; and (iii) the organization verifies media sanitization and disposal actions.		
Physical and Environmental Security (SG.PE)				
SG.PE-1	Physical and Environmental Security Policy and Procedures	SG.PE-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the physical and environmental security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented physical and environmental security policy that addresses— (I) the objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements. SG. PE -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. PE -1.3 Determine if the organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental security policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical and environmental security responsibilities].
SG.PE-2	Physical Access Authorizations	SG.PE-2.1 Determine if: (i) the organization develops lists of personnel with authorized access to facilities containing Smart Grid	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		information systems; (ii) the organization maintains lists of personnel with authorized access to facilities containing Smart Grid information systems; (iii) the organization issues appropriate authorization credential to personnel for facilities containing Smart Grid information systems; and (iv) the organization identifies areas with the facility containing Smart Grid information systems that are publicly accessible. SG.PE-2.2 Determine if: (i) the organization documents designated officials to review and approval access lists for facilities containing Smart Grid information systems; (ii) the organization defines the frequency for review and approval of access lists; (iii) designated officials within the organization review and approve access lists on an organization-defined frequency; and (iv) the designated officials with the organization removes from the access list personnel no longer requiring access to facilities containing Smart Grid information systems.		areas that are publicly accessible and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; and organizational personnel with physical access to Smart Grid information system facility].
SG.PE-3	Physical Access	SG.PE-3.1 Determine if: (i) the organization documents all physical access authorizations for all physical access points to the facility where the Smart Grid information system resides; and (ii) the organization enforces physical access authorizations for all physical access points to the facility where the Smart Grid information system resides. SG.PE-3.2 Determine if the organization verifies individual access authorizations before granting access to the facility. SG.PE-3.3 Determine if the organization controls entry to facilities containing Smart Grid information systems. SG.PE-3.4 Determine if the organization secures keys, combinations, and other physical access devices. SG.PE-3.5 Determine if:	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; Smart Grid information system entry and exit points; procedures addressing physical access control; Smart Grid information system entry and exit points; security plan; list of areas within the facility containing high concentrations of Smart Grid information system components or Smart Grid information system components requiring additional physical protection; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access control responsibilities]. Test: [SELECT FROM: Physical access control capability; and physical access control devices].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization inventories physical access devices on a periodic basis; and (ii) the organization defines the frequency for conducting inventories of physical access devices. SG.PE-3.6 Determine if: (i) the organization defines the frequency of changing combinations, keys, and authorization credentials; (ii) the organization changes combinations, keys, and authorization credentials on an organization-defined frequency; and (iii) the organization changes combinations, keys, and authorization credentials when (a) keys are lost; (b) combinations are compromised; (c) individual credentials are lost; (d) individuals are transferred; and (e) individuals are terminated. SG.PE-3.7 (requirement enhancement 1) Determine if the organization requires physical access mechanisms to Smart Grid information system assets in addition to physical access mechanisms to the facility. SG.PE-3.8 (requirement enhancement 2) Determine if the organization employs hardware to deter unauthorized physical access to Smart Grid information system devices.		
SG.PE-4	Monitoring Physical Access	SG.PE-4.1 Determine if the organization monitors physical access to the Smart Grid information system to detect and respond to physical security incidents. SG.PE-4.2 Determine if: (i) the organization logs physical access to the Smart Grid information system; (ii) the organization defines the frequency to review physical access logs; and (iii) the organization reviews physical access logs on an organization-defined frequency. SG.PE-4.3 Determine if: (i) the organization coordinates results of reviews with the organization's incident response capability; and	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities]. Test: [SELECT FROM: Physical access monitoring capability].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the organization coordinates results of investigations with the organization's incident response capability. SG.PE-4.4 Determine if the organization ensures that investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.		
SG.PE-5	Visitor Control	SG.PE-5.1 Determine if: (i) if the organization documents physical access to the Smart Grid information system; and (ii) the organization controls physical access to the Smart Grid information system by authenticating visitors before authorizing access to the facility. SG.PE-5.2 (requirement enhancement 1) Determine if: (i) the organization documents that visitors are escorted and required to adhere to the organization's security policies and procedures; (ii) the organization escorts visitors as required according to security policies and procedures; and (iii) the organization monitors visitor activity as required according to security policies and procedures.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with visitor access control responsibilities]. Test: [SELECT FROM: Visitor access control capability].
SG.PE-6	Visitor Records	SG.PE-6.1 Determine if the organization maintains visitor access records to the facility that include name and organization of the person visiting. SG.PE-6.2 Determine if the organization maintains visitor access records to the facility that include signature of the visitor. SG.PE-6.3 Determine if the organization maintains visitor access records to the facility that include form of identification. SG.PE-6.4 Determine if the organization maintains visitor access records to the facility that include date of access. SG.PE-6.5 Determine if the organization maintains visitor access records to the facility that include time of entry and departure.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing physical access records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.PE-6.6 Determine if the organization maintains visitor access records to the facility that include purpose of visit. SG.PE-6.7 Determine if the organization maintains visitor access records to the facility that include name and organization of person visited. SG.PE-6.8 Determine if: (i) the organization documents designated officials within the organization to review the access logs after closeout and periodically review visitor access logs based on an organization-defined frequency; and (ii) the organization defines the frequency to review the access logs.		
SG.PE-7	Physical Access Log Retention	SG.PE-7.1 Determine if: (i) the organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy; and (ii) the organization defines the frequency to review all physical access logs based on applicable regulations or by an approved policy.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing physical access records].
SG.PE-8	Emergency Shutoff Protection	SG.PE-8.1 Determine if the organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities to develop physical and environmental protection policies; and organizational personnel with power source emergency shutoff responsibilities].
SG.PE-9	Emergency Power	SG.PE-9.1 Determine if the organization provides an alternate power supply to facilitate an orderly shutdown of noncritical Smart Grid information system components in the event of a primary power source loss. SG.PE-9.2 (requirement enhancement 1) Determine if the organization provides a long-term alternate power supply for the Smart Grid information system that is capable of maintaining minimally required operational	Examine, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; alternate power supply documentation; alternate power test records; and other relevant documents or records]. Test: [SELECT FROM: Uninterruptible power supply; Alternate power supply].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		capability in the event of an extended loss of the primary power source.		
SG.PE-10	Delivery and Removal	SG.PE-10.1 Determine if: (i) the organization defines the types of Smart Grid information system components to be authorized, monitored, and controlled as such components are entering or exiting the facility; (ii) the organization authorizes organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items; (iii) the organization monitors organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items; and (iv) the organization controls organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing delivery and removal of Smart Grid information system components from the facility; security plan; facility housing the Smart Grid information system; records of items entering and exiting the facility; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with responsibilities for controlling Smart Grid information system components entering and exiting the facility]. Test: [SELECT FROM: Process for controlling Smart Grid information system-related items entering and exiting the facility].
SG.PE-11	Alternate Work Site	SG.PE-11.1 Determine if the organization establishes an alternate work site (for example, private residences) with proper equipment and communication infrastructure to compensate for the loss of the primary work site. SG.PE-11.2 Determine if: (i) the organization implements appropriate management security measures at alternate control centers; (ii) the organization implements appropriate operational security measures at alternate control centers; and (iii) the organization implements appropriate technical security measures at alternate control centers.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel using alternate work sites].
SG.PE-12	Location of Smart Grid Information System Assets	SG.PE-12.1 Determine if the organization locates Smart Grid information system assets to minimize potential damage from physical and environmental hazards. SG.PG-12.2 (requirement enhancement 1) Determine if the organization considers the risk associated with physical and environmental hazards when planning new Smart Grid information system facilities or reviewing existing facilities.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing positioning of Smart Grid information system components; documentation providing the location and position of Smart Grid information system components within the facility; physical site planning documents; organizational assessment of risk, contingency plan; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with site selection responsibilities for the facility housing the Smart Grid information system].
Planning (SG.PL)				

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PL-1	Strategic Planning Policy and Procedures	SG.PL-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the planning security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented planning security policy that addresses— (I) the objectives, roles, and responsibilities for the planning security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the planning security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the planning security policy and associated planning protection requirements. SG. PL -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. PL -1.3 Determine if the organization ensures that the planning security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Security planning policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning responsibilities].
SG.PL-2	Smart Grid Information System Security Plan	SG.PL-2.1 Determine if the organization develops a security plan for each Smart Grid information system that: (i) aligns with the organization's enterprise architecture; (ii) explicitly defines the components of the Smart Grid information system; (iii) describes relationships with and interconnections to other Smart Grid information systems; (iv) provides an overview of the security objectives for the Smart Grid information system; (v) describes the security requirements in place or planned for meeting those requirements; and (vi) is reviewed and approved by the management authority prior to plan implementation.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the Smart Grid information system; records of security plan reviews and updates; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security planning and plan implementation responsibilities for the Smart Grid information system].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.PL-2.2 Determine if the organization reviews the security plan for the Smart Grid information system on an organization-defined frequency. SG.PL-2.3 Determine if the organization revises the plan to address changes to the Smart Grid information system/environment of operation or problems identified during plan implementation or security requirement assessments.		
SG.PL-3	Rules of Behavior	SG.PL-3.1 Determine if: (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to Smart Grid information system usage; and (ii) the organization makes readily available a set of rules that describe user responsibilities and expected behavior with regard to Smart Grid information system usage.	Examine	Examine: [SELECT FROM: Security planning policy; procedures addressing rules of behavior for Smart Grid information system users; rules of behavior; and other relevant documents or records].
SG.PL-4	Privacy Impact Assessment	SG.PL-4.1 Determine if the organization conducts a privacy impact assessment on Smart Grid information systems. SG.PL-4.2 Determine if: (i) the privacy impact assessment is reviewed by an organizational management authority; and (ii) the privacy impact assessment is approved by an organizational management authority.	Examine	Examine: [SELECT FROM: Security planning policy; procedures addressing privacy impact assessments on the Smart Grid information system; privacy impact assessment; and other relevant documents or records].
SG.PL-5	Security-Related Activity Planning	SG.PL-5.1 Determine if: (i) the organization plans security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals; and (ii) the organization coordinates security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations organizational assets, or individuals. SG.PL-5.2 Determine if the organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid information system; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
Security Program Management (SG.PM)				
SG.PM-1	Security Policy and Procedures	SG.PM-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the security program security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented security program security policy that addresses— (I) the objectives, roles, and responsibilities for the security program security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the security program security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the security program security policy and associated security program protection requirements. SG. PM -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. PM -1.3 Determine if the organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities for the information security program].
SG.PM-2	Security Program Plan	SG.PM-2.1 Determine if the organization develops and disseminates an organization-wide security program plan that— (i) provides an overview of the requirements for the security program and a description of the security program management requirements in place or planned for meeting those program requirements; (ii) provides sufficient information about the program management requirements to enable an implementation that is compliant with the intent of the plan and a determination of the risk to be incurred if the plan is	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; and other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		implemented as intended; (iii) includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and (iv) is approved by a management authority with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals. SG.PM-2.2 Determine if the organization reviews the organization-wide security program plan on an organization-defined frequency. SG.PM-2.3 Determine if the organization revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments.		Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities for the information security program].
SG.PM-3	Senior Management Authority	SG.PM-3.1 Determine if the organization appoints a senior management authority with the responsibility for the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior management authority position; information security program mission statement; and other relevant documents or records]. Interview: [SELECT FROM: Organizational person appointed to the senior management authority position].
SG.PM-4	Security Architecture	SG.PM-4.1 Determine if the organization develops security architecture with consideration for the resulting risk to: (i) organizational operations; (ii) organizational assets; (iii) individuals; and (iv) other organizations.	Examine	Examine: [SELECT FROM: Information security program policy; security architecture policy; procedures addressing information security-related aspects of security architecture development; system development life cycle documentation; security architecture documentation; enterprise security architecture documentation; and other relevant documents or records].
SG.PM-5	Risk Management Strategy	SG.PM-5.1 Determine if the organization develops a comprehensive strategy to manage Smart Grid information system operational and usage risk to: (i) organizational operations; (ii) organizational assets; (iii) individuals; and (iv) other organizations SG.PM-5.2	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk management strategy development and

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the organization implements that comprehensive risk strategy consistently across the organization.		implementation responsibilities].
SG.PM-6	Security Authorization to Operate Process	SG.PM-6.1 Determine if the organization manages (e.g., documents, tracks, and reports) the security state of organizational information systems through security authorization processes. SG.PM-6.2 Determine if the organization fully integrates the security authorization to operate processes into an organization-wide risk management strategy.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security authorization responsibilities for Smart Grid information systems; and organizational personnel with risk management responsibilities].
SG.PM-7	Mission/Business Process Definition	SG.PM-7.1 Determine if the organization defines mission/business processes that include: (i) consideration for security organizational operations, organizational assets, and individuals; and (ii) the resulting risk to organizational operations, organizational assets, and individuals.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing security categorization of organizational information and Smart Grid information systems; organizational mission/business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with mission/business process definition responsibilities; and organizational personnel with security categorization and risk management responsibilities for the information security program].
SG.PM-8	Management Accountability	SG.PM-8.1 Determine if the organization defines a framework of management accountability that establishes roles and responsibilities to: (i) approve cyber security policy; (ii) assign security roles; and (iii) coordinate the implementation of cyber security across the organization.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing management accountability; information security program plan; security roles and responsibilities; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with management accountability for the information security program].
Personnel Security (SG.PS)				
SG.PS-1	Personnel Security Policy and Procedures	SG.PS-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the personnel security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency—	Examine, Interview	Examine: [SELECT FROM: Personnel security policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(a) a documented personnel security policy that addresses— (I) the objectives, roles, and responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the personnel security policy and associated personnel protection requirements. SG. PS -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. PS -1.3 Determine if the organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.PS-2	Position Categorization	SG.PS-2.1 Determine if: (i) the organization assigns a risk designation to all positions; (ii) the organization establishes screening criteria for individuals filling designated risk positions; (iii) the organization reviews position risk designations; (iv) the organization revises position risk designations; and (v) the organization determines the frequency of the review based on the organization's requirements or regulatory commitments.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing position categorization; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-3	Personnel Screening	SG.PS-3.1 Determine if: (i) the organization screens individuals requiring access to the Smart Grid information system before access is authorized; and (ii) the organization maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-4	Personnel	SG.PS-4.1	Examine, Interview	Examine: [SELECT FROM: Personnel security policy;

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
	Termination	Determine if: (i) the organization revokes logical and physical access to facilities and systems when an employee is terminated; (ii) the organization ensures that all organization-owned property is returned when an employee is terminated; and (iii) the organization-owned documents relating to the Smart Grid information system that are in the employee's possession are transferred to the new authorized owner. SG.PS-4.2 Determine if: (i) the organization defines the time frame to revoke logical and physical access to organizational resources for personnel; and (ii) logical and physical access is terminated at an organization-defined time frame for personnel terminated for cause. SG.PS-4.3 Determine if the organization ensures that during the individuals exit interview, they understand any security constraints imposed by being a former employee and that proper accountability is achieved for all Smart Grid information system-related property.		procedures addressing personnel termination; records of personnel termination actions; and list of Smart Grid information system accounts; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-5	Personnel Transfer	SG.PS-5.1 Determine if: (i) the organization reviews logical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions; and (ii) the organization reviews physical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. SG.PS-5.2 Determine if: (i) the organization defines the time period to review logical and physical access permissions; (ii) the organization completes the logical access permission review within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources; and	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of Smart Grid information system and facility access authorizations; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(iii) the organization completes the physical access permission review within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources.		
SG.PS-6	Access Agreements	SG.PS-6.1 Determine if: (i) the organization completes appropriate agreements for Smart Grid information system access before access is granted; and (ii) the organization ensures the Smart Grid information system access agreements apply to all parties, including third parties and contractors, who require access to the Smart Grid information system. SG.PS-6.2 Determine if: (i) the organization reviews Smart Grid information system access agreements periodically; and (ii) the organization updates Smart Grid information system access agreements periodically. SG.PS-6.3 Determine if the organization requires the signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the Smart Grid information system to which access is authorized.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing access agreements for organizational information and Smart Grid information systems; security plan; access agreements; records of access agreement reviews and updates; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-7	Contractor and Third-Party Personnel Security	SG.PS-7.1 Determine if: (i) the organization enforces Smart Grid information system security requirements for contractor and third-party personnel; and (ii) the organization monitors service provider behavior and compliance to Smart Grid information system security requirements.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing third-party and contractor personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; and third-party providers and contractors].
SG.PS-8	Personnel Accountability	SG.PS-8.1 Determine if the organization employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply. SG.PS-8.2 Determine if the organization ensures that the accountability process complies with applicable federal, state, local, tribal,	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel accountability; rules of behavior; records of personnel disciplinary actions for failure to comply with security policies and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		and territorial laws and regulations.		
SG.PS-9	Personnel Roles	SG.PS-9.1 Determine if the organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.	Examine, Interview	Examine: [SELECT FROM: Personnel roles security policy; procedures addressing personnel roles; third party and contractor policy; third party and contractor standards and procedures; rules of behavior; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; and organizational personnel with third party and contractor security responsibilities].
Risk Management and Assessment (SG.RA)				
SG.RA-1	Risk Assessment Policy and Procedures	SG.RA-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the risk assessment security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented risk assessment security policy that addresses— (I) the objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements. SG. RA -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. RA -1.3 Determine if the organization ensures that the risk assessment security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].
SG.RA-2	Risk Management	SG.RA-2.1	Examine, Interview	Examine: [SELECT FROM: Information security

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
	Plan	Determine if the organization develops a risk management plan. SG.RA-2.2 Determine if: (i) the organization assigns a management authority to review and approve a risk management plan; and (ii) a management authority reviews and approves the risk management plan. SG.RA-2.3 Determine if: (i) the organization's risk-reduction mitigation measures are planned to ensure effectiveness of the organization's risk management plan; (ii) the organization's risk-reduction mitigation measures are implemented to ensure effectiveness of the organization's risk management plan; and (iii) the organization's risk-reduction mitigation results are monitored to ensure effectiveness of the organization's risk management plan.		program policy; risk management policy; procedures addressing risk management plan development and implementation; risk management plan; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk management plan development, implementation, and review responsibilities].
SG.RA-3	Security Impact Level	SG.RA-3.1 Determine if the organization specifies the information and the information system impact levels. SG.RA-3.2 Determine if the organization documents the impact level results (including supporting rationale) in the security plan for information and the information system. SG.RA-3.3 Determine if: (i) the organization defines the frequency for Smart Grid information system and impact level reviews; and (ii) the organization reviews the Smart Grid information system and information impact levels on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; procedures addressing security impact level identification of organizational information and Smart Grid information systems; security planning policy and procedures; security plan; security impact level documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities].
SG.RA-4	Risk Assessment	SG.RA-4.1 Determine if the organization conducts assessments of risk from: (i) the unauthorized access of information and Smart Grid information systems; (ii) use of information and Smart Grid information systems; (iii) disclosure of information and Smart Grid information systems; (iv) disruption of information and Smart Grid information systems;	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(v) modification of information and Smart Grid information systems; and (vi) destruction of information and Smart Grid information systems. SG.RA-4.2 Determine if the organization updates risk assessments on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system or environment of operation, or other conditions that may impact the security of the Smart Grid information system.		
SG.RA-5	Risk Assessment Update	SG.RA-5.1 Determine if the organization updates the risk assessment plan on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system, the facilities where the Smart Grid information system resides, or other conditions that may affect the security or authorization-to-operate status of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].
SG.RA-6	Vulnerability Assessment and Awareness	SG.RA-6.1 Determine if: (i) the organization defines the frequency to monitor and evaluate the Smart Grid information system to identify vulnerabilities; (ii) the organization monitors the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system; and (iii) the organization evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system. SG.RA-6.2 Determine if: (i) the organization analyzes vulnerability scan reports within an organization-defined time frame based on an assessment of risk; and (ii) the organization remediates vulnerabilities within an organization-defined time frame based on an assessment of risk. SG.RA-6.3 Determine if the organization shares information obtained from the vulnerability scanning process with designated	Examine, Interview, Test	Examine: [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; security plan; list of Smart Grid information system components for vulnerability scanning; list of vulnerabilities scanned; personnel access authorization list; authorization credentials; access authorization records; vulnerability scanning tools and techniques documentation; patch and vulnerability management records; records of updates to vulnerabilities scanned; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment and vulnerability scanning responsibilities]. Test: [SELECT FROM: Vulnerability scanning capability and associated scanning tools].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		personnel throughout the organization to help eliminate similar vulnerabilities in other Smart Grid information systems. SG.RA-6.4 Determine if the organization updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy. SG.RA-6.5 Determine if: (i) the organization defines the frequency to update the list of Smart Grid information system vulnerabilities; and (ii) the organization updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported. SG.RA-6.6 (requirement enhancement 1) Determine if the organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned. SG.RA-6.7 (requirement enhancement 2) Determine if: (i) the organization defines the list of Smart Grid information system components to which privileged access is authorized for selected vulnerability scanning activities; and (ii) the organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.		
Smart Grid Information System and Services Acquisition (SG.SA)				
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	SG.SA-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the Smart Grid information system and services acquisition security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented Smart Grid information system and services acquisition security policy that addresses— (I) the objectives, roles, and responsibilities for the Smart Grid information system and	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with system and services acquisition responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		services acquisition security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the Smart Grid information system and services acquisition security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the Smart Grid information system and services acquisition security policy and associated Smart Grid information system and services acquisition protection requirements. SG. SA -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. SA -1.3 Determine if the organization ensures that the Smart Grid information system and services acquisition security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.SA-2	Security Policies for Contractors and Third Parties	SG.SA-2.1 Determine if: (i) the organization identifies external suppliers and contractors that have an impact on the security of Smart Grid information systems; and (ii) the organization's external suppliers and contractors that have an impact on the security of Smart Grid information systems meet the organization's policy and procedures. SG.SA-2.2 Determine if: (i) the organization establishes procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract; and (ii) the organization documents procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy and procedures; personnel security policy; procedures addressing personnel sanctions; third party policy; third party standards and procedures; rules of behavior; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with third party and contractor security responsibilities; and organizational personnel with system and services acquisition responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		contract.		
SG.SA-3	Life-Cycle Support	SG.SA-3.1 Determine if the organization manages the Smart Grid information system using a system development lifecycle methodology that includes security.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; Smart Grid information system development life cycle documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information security and system life cycle development responsibilities].
SG.SA-4	Acquisitions	SG.SA-4.1 Determine if the organization includes security requirements in Smart Grid information system acquisition contracts in accordance with applicable laws, regulations, and organization-defined security policies.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for Smart Grid information systems or services; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].
SG.SA-5	Smart Grid Information System Documentation	SG.SA-5.1 Determine if the Smart Grid information system documentation includes: (i) how to configure the Smart Grid information system and the Smart Grid information system's security features; (ii) install the Smart Grid information system and the Smart Grid information system's security features; and (iii) use the Smart Grid information system and the Smart Grid information system's security features. SG.SA-5.2 Determine if the organization obtains from the contractor/third-party, information describing the functional properties of the security controls employed within the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system documentation; Smart Grid information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent Smart Grid information system documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the Smart Grid information system; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities; and organizational personnel operating, using, and/or maintaining the Smart Grid information system].
SG.SA-6	Software License Usage Restrictions	SG.SA-6.1 Determine if the organization uses software and associated documentation in accordance with contract agreements and copyright laws. SG.SA-6.2	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; and other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if the organization controls the use of software and associated documentation protected by quantity licenses and copyrighted material.		Interview: [SELECT FROM: Organizational personnel with Smart Grid information system administration responsibilities; and organizational personnel operating, using, and/or maintaining the Smart Grid information system].
SG.SA-7	User-Installed Software	SG.SA-7.1 Determine if the organization establishes policies and procedures to manage user installation of software.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the Smart Grid information system; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system administration responsibilities; and organizational personnel operating, using, and/or maintaining the Smart Grid information system].
SG.SA-8	Security Engineering Principles	SG.SA-8.1 Determine if the organization applies security engineering principles in the specification of any Smart Grid information system; design of any Smart Grid information system; development of any Smart Grid information system; and implementation of any Smart Grid information system. SG.SA-8.2 Determine if the organization's security engineering principles include ongoing secure development education requirements for all developers involved in the Smart Grid information system. SG.SA-8.3 Determine if the organization's security engineering principles include specification of a minimum standard for security. SG.SA-8.4 Determine if the organization's security engineering principles include specification of a minimum standard for privacy. SG.SA-8.5 Determine if the organization's security engineering principles include creation of a threat model for a Smart Grid information system. SG.SA-8.6 Determine if the organization's security engineering principles include updating of product specifications to include mitigations for threats discovered during threat modeling.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the Smart Grid information system; Smart Grid information system design documentation; security requirements and security specifications for the Smart Grid information system; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system design, development, implementation, and modification responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		SG.SA-8.7 Determine if the organization's security engineering principles include use of secure coding practices to reduce common security errors. SG.SA-8.8 Determine if the organization's security engineering principles include testing to validate the effectiveness of secure coding practices. SG.SA-8.9 Determine if the organization's security engineering principles include performance of a final security audit prior to authorization to operate to confirm adherence to security requirements. SG.SA-8.10 Determine if the organization's security engineering principles include c creation of a documented and tested security response plan in the event vulnerability is discovered. SG.SA-8.11 Determine if the organization's security engineering principles include creation of a documented and tested privacy response plan in the event vulnerability is discovered. SG.SA-8.12 Determine if the organization's security engineering principles include performance of a root cause analysis to understand the cause of identified vulnerabilities.		
SG.SA-9	Developer Configuration Management	SG.SA-9.1 Determine if the organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that manages and controls changes to the Smart Grid information system during design, development, implementation, and operation. SG.SA-9.2 Determine if the organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that tracks security flaws. SG.SA-9.3 Determine if the organization requires that Smart Grid information system developers/integrators document and	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer/integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; and other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; and organization personnel with configuration management responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		implement a configuration management process that includes organizational approval of changes.		
SG.SA-10	Developer Security Testing	SG.SA-10.1 Determine if the Smart Grid information system developer creates a security test and evaluation plan. SG.SA-10.2 Determine if: (i) the developer submits the plan to the organization for approval; and (ii) the developer implements the plan once written approval is obtained. SG.SA-10.3 Determine if: (i) the developer documents the results of the testing and evaluation; and (ii) the developer submits them to the organization for approval. SG.SA-10.4 Determine if the organization does not perform developmental security tests on the production Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer/integrator security testing; acquisition contracts and service level agreements; Smart Grid information system developer/integrator security test plans; records of developer/integrator security testing results for the Smart Grid information system; security flaw tracking records; security test and evaluation plan; security test and evaluation results report; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with developer security testing responsibilities].
SG.SA-11	Supply Chain Protection	SG.SA-11.1 Determine if: (i) the organization defines the measures to be employed to protect again supply chain threats; and (ii) the organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against: (a) organizations, that provide products or services to the organization; (b) people, that provide products or services to the organization; (c) information, used to provide products or services to the organization; and (d) resources, used to provide products or services to the organization.	Examine	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; Smart Grid information system development life cycle documentation; due diligence reviews documentation; and other relevant documents or records].
Smart Grid Information System and Communication Protection (SG.SC)				
SG.SC-1	System and Communication Protection Policy and Procedures	SG.SC-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the Smart Grid information system and communication protection security policy and procedures;	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy, procedures, forms, memos, and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with system and communications protection

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented Smart Grid information system and communication protection security policy that addresses— (I) the objectives, roles, and responsibilities for the Smart Grid information system and communication protection security program as it relates to protecting the organization's personnel and assets; and (II) the scope of the Smart Grid information system and communication protection security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the Smart Grid information system and communication protection security policy and associated Smart Grid information system and communication protection requirements. SG. SC -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. SC -1.3 Determine if the organization ensures that the Smart Grid information system and communication protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		responsibilities].
SG.SC-2	Communications Partitioning	SG.SC-2.1 Determine if the Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing communication partitioning; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [Separation of communications for telemetry/data acquisition services from management functionality.]
SG.SC-3	Security Function	SG.SC-3.1	Examine, Test	Examine: [SELECT FROM: System and

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
	Isolation	Determine if: (i) the organization defines the security functions of the Smart Grid information system; and (ii) the Smart Grid information system isolates security functions from non-security functions.		communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Separation of security functions from nonsecurity functions within the Smart Grid information system].
SG.SC-4	Information Remnants	SG.SC-4.1 Determine if the Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing information remnants; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system for unauthorized and unintended transfer of information via shared system resources].
SG.SC-5	Denial-of-Service Protection	SG.SC-5.1 Determine if: (i) the organization documents a defined list of denial-of-service attacks against the Smart Grid information systems; and (ii) the Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing denial of service protection; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system for protection against or limitation of the effects of denial of service attacks].
SG.SC-6	Resource Priority	SG.SC-6.1 Determine if the Smart Grid information system prioritizes the use of resources.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing prioritization of Smart Grid information system resources; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing resource allocation capability].
SG.SC-7	Boundary Protection	SG.SC-7.1 Determine if: (i) the organization defines the external boundary of the Smart Grid information system; and	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the organization defines key internal boundaries of the Smart Grid information system. SG.SC-7.2 Determine if: (i) the Smart Grid information system monitors communications at the external boundary of the system and at key internal boundaries within the system; and (ii) the Smart Grid information system controls communications at the external boundary of the system and at key internal boundaries within the system. SG.SC-7.3 Determine if the Smart Grid information system connects to external networks or Smart Grid information systems only through managed interfaces consisting of boundary protection devices in accordance with the organizational security architecture. SG.SC-7.4 Determine if the managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information. SG.SC-7.5 Determine if: (i) the organization defines the mediation necessary for public access to the organization's internal Smart Grid information system networks; and (ii) the organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated. SG.SC-7.6 (requirement enhancement 1) Determine if: (i) the Smart Grid information system denies network traffic by default; and (ii) the Smart Grid information system allows network traffic by exception. SG.SC-7.7 (requirement enhancement 2) Determine if the Smart Grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination. SG.SC-7.8 (requirement enhancement 3)		of mediation vehicles for allowing public access to the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; traffic flow policy; Smart Grid information system security architecture; boundary protection hardware and software; records of traffic flow policy exceptions; Smart Grid information system architecture; Smart Grid information system configuration settings and associated documentation; facility communications and wiring diagram; Smart Grid information system architecture and configuration documentation; Smart Grid information system audit records; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific boundary protection responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing access controls for public access to the organization's internal networks; Managed interfaces implementing organizational traffic flow policy; Automated mechanisms supporting the fail-safe boundary protection capability within the Smart Grid information system; and Mechanisms implementing managed interfaces within Smart Grid information system boundary protection devices.

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		Determine if: (i) communications to/from Smart Grid information system components are restricted to specific components in the Smart Grid information system; and (ii) communications are restricted to/from any non-Smart Grid information system unless separated by a controlled logical/physical interface.		
SG.SC-8	Communication Integrity	SG.SC-8.1 Determine if the Smart Grid information system protects the integrity of electronically communicated information. SG.SC-8.2 (requirement enhancement 1) Determine if the organization employs cryptographic mechanisms to ensure integrity of Smart Grid information system information.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing communication integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Communication integrity capability within the Smart Grid information system; and Cryptographic mechanisms implementing communication integrity capability within the Smart Grid information system].
SG.SC-9	Communication Confidentiality	SG.SC-9.1 Determine if the Smart Grid information system protects the confidentiality of communicated information. SG.SC-9.2 (requirement enhancement 1) Determine if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission of Smart Grid information system information.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing communication confidentiality; Smart Grid information system design documentation; Smart Grid information system communications hardware and software or Protected Distribution System protection mechanisms; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Cryptographic mechanisms implementing transmission confidentiality capability within the Smart Grid information system; and Communication confidentiality capability within the Smart Grid information system].
SG.SC-10	Trusted Path	SG.SC-10.1 Determine if: (i) the Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system; and (ii) the Smart Grid information system documents trusted communications path between the user and the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing trusted communications paths; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; assessment results from independent, testing organizations; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing trusted communications paths within

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				the Smart Grid information system].
SG.SC-11	Cryptographic Key Establishment and Management	SG.SC-11.1 Determine if: (i) the organization establishes cryptographic keys for required cryptography employed within the Smart Grid information system; and (ii) the organization manages cryptographic keys for required cryptography employed within the Smart Grid information system. SG.SC-11.2 (requirement enhancement 1) Determine if the organization maintains availability of information in the event of the loss of cryptographic keys by users.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for cryptographic key establishment or management]. Test: [SELECT FROM: Automated mechanisms implementing cryptographic key management and establishment within the Smart Grid information system].
SG.SC-12	Use of Validated Cryptography	SG.SC-12.1 Determine if all cryptography and other security functions are NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; cryptographic module validation certificates; cryptographic module security policy; and other relevant documents or records].
SG.SC-13	Collaborative Computing	SG.SC-13.1 Determine if: (i) the organization develops a collaborative computing policy; (ii) the organization disseminates a collaborative computing policy on an organization-defined frequency; (iii) the organization periodically reviews the collaborative computing policy on an organization-defined frequency; and (iv) the organization periodically updates the collaborative computing policy on an organization-defined frequency.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]
SG.SC-14	Transmission of Security Parameters	SG.SC-14.1 Determine if the Smart Grid information system reliably associates security parameters with information exchanged between the enterprise information systems and the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission of security parameters; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Test: [SELECT FROM: Automated mechanisms supporting reliable transmission of security parameters between Smart Grid information systems].
SG.SC-15	Public Key Infrastructure Certificates	SG.SC-15.1 Determine if (i) the organization defines a certificate policy for issuing public key certificates for Smart Grid information systems that implement a public key infrastructure; and (ii) the organization issues public key certificates under the organization-defined certificate policy or obtains public key certificates under a certificate policy from an approved service provider.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; results of public key infrastructure audit; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with public key infrastructure certificate issuing responsibilities].
SG.SC-16	Mobile Code	SG.SC-16.1 Determine if: (i) the organization establishes usage restrictions for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; and (ii) the organization establishes implementation guidance for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously. SG.SC-16.2 Determine if the organization: (i) documents the use of mobile code within the Smart Grid information system; (ii) monitors the use of mobile code within the Smart Grid information system; and (iii) manages the use of mobile code within the Smart Grid information system. SG.SC-16.3 Determine if: (i) the organization documents a management authority to authorize the use of mobile code; and (ii) a management authority authorizes the use of mobile code.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; acquisition documentation; acquisition contracts for Smart Grid information systems or services; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with mobile code management responsibilities; and organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities]. Test: [SELECT FROM: Mobile code authorization and monitoring capability for the organization; Automated mechanisms implementing mobile code detection and inspection capability; Automated mechanisms preventing download and execution of prohibited mobile code; and Automated mechanisms preventing mobile code execution within the Smart Grid information system].
SG.SC-17	Voice-Over Internet Protocol	SG.SC-17.1 Determine if: (i) the organization establishes usage restrictions for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; and	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; and relevant documents or records]. Interview: [SELECT FROM: Organizational personnel

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(ii) the organization establishes implementation guidance for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously. SG.SC-17.2 Determine if the organization: (i) authorizes the use of VoIP within the Smart Grid information system; (ii) monitors the use of VoIP within the Smart Grid information system; and (iii) controls the use of VoIP within the Smart Grid information system.		with VoIP authorization and monitoring responsibilities]. Test: [SELECT FROM: VoIP authorization and monitoring capability for the organization].
SG.SC-18	System Connections	SG.SC-18.1 Determine if: (i) the organization identifies all external Smart Grid information system and communication connections; and (ii) the organization protects all external Smart Grid information system and communication connections from tampering or damage.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Access control policy; procedures addressing Smart Grid information system connections; Smart Grid information system interconnection security agreements; security plan; Smart Grid information system design documentation; security assessment report; plan of action and milestones; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].
SG.SC-19	Security Roles	SG.SC-19.1 Determine if: (i) if the Smart Grid information system design specifies the security roles and responsibilities for the users of the Smart Grid information system; and (ii) the Smart Grid information system implementation specifies the security roles and responsibilities for the users of the Smart Grid information system	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system roles and responsibilities documentation; list of personnel with security role and responsibility assignments; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information security roles and responsibilities].
SG.SC-20	Message Authenticity	SG.SC-20.1 Determine if the Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Transmission integrity capability within the Smart Grid information system;

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				Cryptographic mechanisms implementing transmission integrity capability within the Smart Grid information system; and Transmission integrity capability within the Smart Grid information system].
SG.SC-21	Secure Name/Address Resolution Service	SG.SC-21.1 Determine if the organization configures systems to provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries. SG.SC-21.2 Determine if: (i) the organization configures systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces; and (ii) the organization configures systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, enables verification of a chain of trust among parent and child domains (if child supports secure resolution services).	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing secure name/address resolution service (authoritative source); and Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services].
SG.SC-22	Fail in Known State	SG.SC-22.1 Determine if: (i) the known states for defined failures are determined for the Smart Grid information system; (ii) the types of failures are defined for which the Smart Grid information system should fail to the known-state; (iii) the state information for the Smart Grid information system that should be preserved in the event of a system failure is defined; (iv) the Smart Grid information system fails to a known-state for defined failures; and (v) the Smart Grid information system preserves the system state in the event of a system failure.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing Smart Grid information system failure; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of failures requiring Smart Grid information system to fail in a known state; state information to be preserved in system failure; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing fail-in-known-state capability].
SG.SC-23	Thin Nodes	SG.SC-23.1 Determine if the Smart Grid information system employs processing components that have minimal functionality and data storage.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of thin nodes; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]
SG.SC-24	Honeypots	SG.SC-24.1 Determine if the Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of:	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of honeypots; access control policy and procedures; boundary protection procedures; Smart

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) detecting; (ii) deflecting; (iii) analyzing; and (iv) tracking attacks.		Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records].
SG.SC-25	Operating System-Independent Applications	SG.SC-25.1 Determine if: (i) the organization defines applications that are operating system-independent; and (ii) the Smart Grid information system includes organization-defined applications.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing operating system-independent applications; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of operating system-independent applications; and other relevant documents or records]
SG.SC-26	Confidentiality of Information at Rest	SG.SC-26.1 Determine if the Smart Grid information system employs cryptographic mechanisms for all critical security parameters (e.g., cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing protection of information at rest; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; and other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing confidentiality and integrity protections for information at-rest; and Cryptographic mechanisms implementing confidentiality and integrity protections for information at-rest].
SG.SC-27	Heterogeneity	SG.SC-27.1 Determine if the organization employs diverse technologies in the implementation of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of technologies deployed in the Smart Grid information system; acquisition documentation; acquisition contracts for Smart Grid information system components or services; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system acquisition, development, and implementation responsibilities].
SG.SC-28	Virtualization Technique	SG.SC-28.1 Determine if the organization employs virtualization techniques to present gateway components into Smart Grid information system environments as other types of components, or components with differing configurations.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system architecture; list of virtualization techniques to

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
				be employed for organizational Smart Grid information systems; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for implementing approved virtualization techniques for Smart Grid information systems].
SG.SC-29	Application Partitioning	SG.SC-29.1 Determine if the Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing separation of user functionality and system management functionality; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Separation of user functionality from Smart Grid information system management functionality].
SG.SC-30	Information System Partitioning	SG.SC-30.1 Determine if the organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments).	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system architecture; list of Smart Grid information system physical domains (or environments); Smart Grid information system facility diagrams; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel installing, configuring, and/or maintaining the Smart Grid information system].
System and Information Integrity (SG.SI)				
SG.SI-1	System and Information Integrity Policy and Procedures	SG.SI-1.1 Determine if: (i) the organization defines the frequency of reviews and updates to the Smart Grid information system and information integrity security policy and procedures; (ii) the organization develops, implements, reviews, and updates on an organization-defined frequency— (a) a documented Smart Grid information system and information integrity security policy that addresses— (I) the objectives, roles, and responsibilities for the Smart Grid information system and information integrity security program as it	Examine, Interview	Examine: [SELECT FROM: System and information integrity policy and procedures; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with system and information integrity responsibilities].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		relates to protecting the organization's personnel and assets; and (II) the scope of the Smart Grid information system and information integrity security program as it applies to all of the organizational staff, contractors, and third parties; and (b) procedures to address the implementation of the Smart Grid information system and information integrity security policy and associated Smart Grid information system and information integrity protection requirements. SG. SI -1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG. SI -1.3 Determine if the organization ensures that the Smart Grid information system and information integrity security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.SI-2	Flaw Remediation	SG.SI-2.1 Determine if: (i) the organization identifies Smart Grid information system flaws; (ii) the organization reports Smart Grid information system flaws; and (iii) the organization corrects Smart Grid information system flaws. SG.SI-2.2 Determine if the organization tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation. SG.SI-2.3 Determine if the organization incorporates flaw remediation into the organizational configuration management process.	Examine, Interview	Examine: [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the Smart Grid information system; list of recent security flaw remediation actions performed on the Smart Grid information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct Smart Grid information system flaws); test results from the installation of software to correct Smart Grid information system flaws; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with flaw remediation responsibilities].
SG.SI-3	Malicious Code and Spam Protection	SG.SI-3.1 Determine if:	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing malicious code

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		(i) the organization implements malicious code protection mechanisms; and (ii) the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. SG.SI-3.2 Determine if the Smart Grid information system prevents users from circumventing malicious code protection capabilities.		protection; malicious code protection mechanisms; records of malicious code protection updates; procedures addressing spam protection; spam protection mechanisms; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with malicious code protection responsibilities; and organizational personnel with spam protection responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing malicious code protection capability; and Automated mechanisms implementing spam detection and handling capability].
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	SG.SI-4.1 Determine if the organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors.	Examine, Interview	Examine: [SELECT FROM: System and information integrity policy; procedures addressing Smart Grid information system monitoring tools and techniques; Smart Grid information system design documentation; Smart Grid information system monitoring tools and techniques documentation; Smart Grid information system configuration settings and associated documentation; techniques; documentation providing evidence of testing intrusion monitoring tools; Smart Grid information system monitoring tools and techniques documentation; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system monitoring responsibilities].
SG.SI-5	Security Alerts and Advisories	SG.SI-5.1 Determine if the organization receives Smart Grid information system security alerts, advisories, and directives from external organizations. SG.SI-5.2 Determine if: (i) the organization generates internal security alerts, advisories, and directives as deemed necessary; and (ii) the organization disseminates internal security alerts, advisories, and directives as deemed necessary.	Examine, Interview	Examine: [SELECT FROM: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; records of security alerts and advisories; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security alert and advisory responsibilities; and organizational personnel implementing, operating, maintaining, administering, and using the Smart Grid information system].

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SI-6	Security Functionality Verification	SG.SI-6.1 Determine if: (i) the organization defines the appropriate conditions, including at the Smart Grid information system start up and restart, for verify the correct operation of security functions; (ii) the organization defines the frequency for periodic verification of security functions; (iii) the organization defines Smart Grid information system responses and alternative action(s) to anomalies discovered during security function verification; (iv) the Smart Grid information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency; and (v) the Smart Grid information system responds to security function anomalies in accordance with organization-defined responses and alternative action(s). SG.SI-6.2 Determine if the Smart Grid information system notifies the management authority when anomalies are discovered.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing security function verification; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; automated security test results; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security functionality verification responsibilities; and organizational personnel with information security responsibilities]. Test: [SELECT FROM: Security function verification capability; and Automated mechanisms implementing alerts and/or notifications for failed security tests].
SG.SI-7	Software and Information Integrity	SG.SI-7.1 Determine if: (i) the Smart Grid information system monitors unauthorized changes to software and information; and (ii) the Smart Grid information system detects unauthorized changes to software and information. SG.SI-7.2 (Requirement enhancement 1) Determine if: (i) the organization reassesses the integrity of software by performing on an organization-defined frequency integrity scans of the Smart Grid information system; (ii) the organization reassesses the integrity of information by performing on an organization-defined frequency integrity scans of the Smart Grid information system; and (iii) the organization defines the frequency of the integrity scans of the Smart Grid information systems.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing software and information integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; Smart Grid information system component packaging; and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security functionality verification responsibilities; organizational personnel with software integrity responsibilities; organization responsibility with change management responsibilities; and organizational personnel with information security responsibilities]. Test: [SELECT FROM: Software integrity protection and verification capability].
SG.SI-8	Information Input Validation	SG.SI-8.1 Determine if: (i) the Smart Grid information system employs mechanisms to check information for accuracy; (ii) the Smart Grid information system employs mechanisms	Examine, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing information accuracy, completeness, validity and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for

Smart Grid Cyber Security Requirement		Assessment Objective	Assessment Method	Potential Assessment Object(s)
		to check information for completeness; (iii) the Smart Grid information system employs mechanisms to check information for validity; and (iv) the Smart Grid information system employs mechanisms to check information for authenticity.		automated tools and applications to verify accuracy, completeness, validity and authenticity of information; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system capability for checking accuracy, completeness, validity, and authenticity of information inputs].
SG.SI-9	Error Handling	SG.SI-9.1 Determine if the Smart Grid information system identifies error conditions. SG.SI-9.2 Determine if: (i) the organization defines sensitive or potentially harmful information that should not be contained in error messages; and (ii) the Smart Grid information system generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.	Examine, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing Smart Grid information system error handling; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; and other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system error handling capability].